Microlog Microfiche Collection
Resolution Chart

Copyright

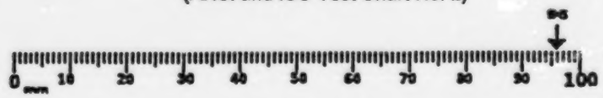
Copyright for the ***contents*** of this microfiche is held by the publisher of the original document. Please contact the original publisher for guidance in all copyright matters. Copyright in this ***microfiche edition*** is held by Micromedia Limited.

Quality of the Microfiche Reproduction

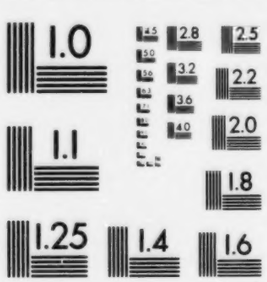
Micromedia Limited maintains the highest standards for micrographic reproduction. Attempts are made to obtain the best quality print version to microfilm. However, there are some printing styles, colours and graphic layout styles (including maps, graphs and tables) which do not reproduce well. Because of the value of the original document, Micromedia has filmed it recognizing that it may not be as easy to read as the original document.

Some pages have been filmed twice to improve the clarity of the reproduction. Consult both reproductions to ensure that all of the original text is read.

Microcopy Resolution Test Chart
National Bureau of Standards
Standard Reference Material 1010a
(ANSI and ISO Test Chart No. 2)



PM-1 3½"x4" PHOTOGRAPHIC MICROCOPY TARGET
NBS 1010a ANSI/ISO #2 EQUIVALENT



MS109

24x

micromedia
a division of IHS Canada

20 Victoria Street, Toronto, ON M5C 2N8
Tel.: (416) 362-5211
Toll free: 1-800-387-2689
Fax: (416) 362-6161

Collection MICROLOG sur Micromédia
Tableau de résolution

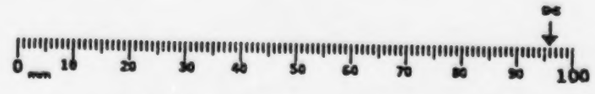
Droits d'auteurs

Les droits d'auteurs du conenu de cette microfiche sont détenus par l'éditeur du document original. Veuillez communiquer avec celui-ci pour obtenir des renseignements sur tout ce qui touche les droits d'auteurs. Les droits d'auteurs de cette édition sur microfiche sont détenus par Micromédia Limitée.

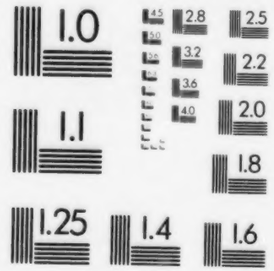
Qualité de reproduction sur microfiche

Micromédia Limitée maintient les normes de reproduction micrographique les plus élevées. Elle fait tout son possible pour obtenir la version sur papier à reproduire sur microfiche de la meilleure qualité possible. Cependant, certains styles d'imprimerie, de couleurs et de style de mise en page graphique (incluant des cartes, des grahiques et des tableaux) se reproduisent mal. En raison de la valeur du document original, Micromédia l'a reproduit tout en reconnaissant qu'il ne sera peut-être pas aussi lisable que le document original.

Tableau de résolution micrographique
National Bureau of Standards
Standard Reference Material 1010a
(ANSI and ISO Test Chart No. 2)



PM-1 3½"x4" PHOTOGRAPHIC MICROCOPY TARGET
NBS 1010a ANSI/ISO #2 EQUIVALENT



MS109

24x

micromedia
a division of IHS Canada

20 Victoria Street, Toronto, ON M5C 2N8
Tel.: (416) 362-5211
Toll free: 1-800-387-2689
Fax: (416) 362-6161

Cryptography Policy Discussion Paper: Analysis of submissions

Prepared by

AEPOS Technologies Corporation

PREPARED FOR : Industry Canada

ORIGINATOR : AEPOS Technologies Corporation
116 Albert St. Suite 601
Ottawa, Ontario
K1P 5G3

DATE: 11th June, 1998

100-06701/

This publication is also available electronically on the World Wide Web at the following address:
http://strategis.ic.gc.ca/crypto

This publication is also available in alternative formats on request.
See distribution contact numbers listed below.

For additional copies of this publication, please contact:

Donna Emmett
Task Force on Electronic Commerce
Industy Canada
300 Slater Street, Room 2022A
Ottawa, Ontario
K1A 0C8

Tel.: (613) 990-9233
Fax: (613) 941-0178
Email: emmett.donna@ic.gc.ca

Michael Harrop may be contacted at:

AEPOS Technologies Corporation
116 Albert St., Suite 601
Ottawa, Ontario
K1P 5G3

Tel.: (613) 599-5905
Fax: (613) 599-4681
Email: mharrop@bigfoot.com

©Her Majesty the Queen in Right of Canada (Industry Canada) 1998
Cat. No.C2-336/2-1998
ISBN 0-662-63949-9

Table of Contents

Introduction 1

General observations on the comments received and the process of analysis 3

Analysis of responses 5
- Part 1: Summary of quantitative results 5
  - Overall position towards controls on cryptography 5
  - Encryption of stored data 6
  - Encryption of real-time communication data 7
  - Export controls 9
- Part 2: Review of narrative responses 10
  - General observations 10
  - Mandatory key recovery/key escrow issues 10
  - Access to stored data 12
  - Real-time communications data recovery 12
  - Cost issues 13
  - Privacy issues 13
  - Law enforcement issues 14
  - Export Controls 16
  - The need for suppliers and carriers to be treated equally 17
  - Legislation, regulation and Charter issues 17
  - Other issues 18
  - Conclusions and possible follow-on actions 19
- Part 3: Suggestions for expediting the rollout of secure electronic commerce 20
  - Legal issues 20
  - Trusted Third Parties 21
  - Lead by example 21
  - Security for electronic commerce 21
  - Role of government in promoting the electronic services 22
  - International issues 23

Closing remarks 24

Annex A: Resolution of the Association of Canadian Chiefs of Police, August 1997 25

Annex B: Index of Submissions to the Discussion Paper 26

Introduction

This report contains an analysis of the responses to the Industry Canada discussion paper *A Cryptography Policy Framework for Electronic Commerce* (February 1998). The paper was released for public comment on 21 February, 1998 with a comment closing date of 21st April, 1998. A total of 189 responses were received by the closing date. A further 15 responses were received between the closing date and 22nd May.

In addition to comments in response to the discussion paper, responses included requests for more information, e-mails and letters acknowledging receipt of the discussion paper, e-mail advertising (spam), messages that appeared not to have any relevance to the topic (such as a request for help with a consumer problem), duplicate copies of submissions submitted by different delivery mechanisms and at different times, and faxed cartoons. These responses were not included in quantitative assessment or the analysis.

Late contributions are not included in the statistical analysis but the comments have been considered and taken into account in the evaluation process.

The overall count of submissions was as follows:

Total on-time responses:	189
Responses not analysed (see above):	53
On-time submissions analysed:	136
Late submissions:	15
Total responses (as of 22nd May, 1998):	204

The submissions received represent a broad cross section of interest. In addition to 77 responses from private individuals and academics, submissions were received from 13 supplier/manufacturer companies, 18 law enforcement agencies from all parts of the country, four public sector agencies (including the offices of three Information and Privacy Commissioners), five industry associations, five privacy/human rights organizations, five carriers or carrier associations, five consultants and four other organizations. The carrier associations represented all provincial telephone companies plus some of the wireless companies. The industry associations included representation for Canadian financial institutions across the country, 110 Internet service providers, over 3500 manufacturing and exporting companies, the telecommunications user interests of over 400 businesses, governments and healthcare providers with an aggregate total of over 2 million employees, and over 1300 computer hardware, software and service companies with revenues in excess of $45 billion and over 290,000 employees.

A number of submissions arrived indirectly. These included 14 individual letters that were addressed to Industry Canada as responses but which accompanied the Electronic Frontier Canada submission and some submissions from law enforcement agencies which were addressed to the RCMP, the Ottawa Carleton Police Force and the Ontario Solicitor General, rather than Industry Canada. Each of these contributions has been included as a distinct submission. In addition, a single letter signed by 20 international organizations concerned with defending civil liberties and human rights on the Internet, was included with the Electronic Frontier Canada submission. For analysis purposes, this letter was considered as part of the Electronic Frontier Canada submission, rather than being identified as a separate contribution.

Submissions varied in length and detail from very short individual e-mails that protested about any kind of government control to very substantial formal submissions developed by committee. All responses judged to have any relevance to the discussion have been included in the analysis regardless of origin, tenor or level of detail.

Eight of the contributions, including that of one carrier association, expressed concern and disappointment that the discussion paper seemed slanted towards meeting law enforcement needs to access electronic information. It was suggested that there should be more emphasis on the positive aspects of cryptography and on protecting individual rights than on placing restrictions on individuals and businesses. Several comments were also made on the use of the term *lawful access* in the policy paper, observing that this is a euphemism for law enforcement access, since all crypto systems allow lawful access to their legitimate users.

A number of respondents thanked Industry Canada for presenting the issues in a public discussion paper and for giving them the opportunity to participate in the discussions. The thoroughness of the coverage of the discussion paper was frequently praised. Some respondents offered clarifications, elaborations and corrections and a number of respondents protested that the review period had been insufficiently long. Overall, the comments on the discussion paper and the process were quite favourable with most respondents appreciating the opportunity to participate in this policy development process.

General observations on the comments received and the process of analysis

Before moving on to analysis of the responses on the individual questions, a few words on the general approach and process used to evaluate the comments are in order.

As noted above, the responses varied considerably in detail and coverage. Some responses were from individuals, some from companies, some from public sector agencies, some from interest groups and associations and some from industry associations. Some responses directly addressed the issues of the discussion paper and offered answers to the questions raised while others were more of the nature of issues papers. Some responses were broad-ranging while others addressed only a single issue or a subset of the issues raised in the discussion paper. Some of the submissions provided very direct and to-the-point responses while others provided responses that were sometimes heavily masked by accompanying commentary. However, overall the responses represent a substantial amount of collective thought and effort and provide significant insight into the issues under discussion together with the considered opinions of a broad constituency. Although the analysis provided here can offer an overview into the collective thinking and opinions, the individual submissions themselves must stand as the primary response to the discussion paper.

The analysis provided in this report is partly quantitative, partly qualitative. For the most part, the submissions received comprised narrative responses to relatively open questions. Unfortunately there is no reliable or accepted way to quantitatively evaluate responses to open questions. Even the responses to the relatively closed questions (as represented by the policy options suggested under the issues of how to address encryption of stored data, realtime data and export controls), often tended to be open responses, rather than simple selection of one of the options. Thus even with the closed questions it was often necessary to interpret a narrative response as indicating one (or perhaps none) of the indicated options. Responses that said "not option 2 or 3", rather than simply indicating a preference for option 1 presented yet another challenge. Overall, the approach taken to evaluate the responses to the closed questions was to tally the responses by contributing group under each of the question headings. Where no preferred option was indicated, or where the respondent failed to comment on the issue, the contribution was excluded from the tally on that particular question. (Not all submissions responded on all the issues). The resulting assessment of the responses to the closed questions is believed to provide a reasonably accurate quantitative assessment.

Presentation of the qualitative information is much more difficult as it inevitably involves a degree of subjectivity. The approach selected was to search for those points most frequently raised and to provide a summary of the issues identified. In addition, and most subjective of all, points which, although perhaps not frequently mentioned, but which appear

to have particular relevance to the debate, or perhaps offer some new insight, have been included where appropriate.

Both quantitative and qualitative results are of value but each provides a different insight into the results. The quantitative results can provide an overall picture of stated preferences but the qualitative results, represented by the narrative responses, provide the rationale behind the stated preferences and also set out the likely implications of taking a particular direction.

Lastly, for purposes of analysis, the responses were divided into the following categories:

Individual;
Industry Associations;
Law enforcement and national security;
Privacy and human rights groups (excluding public sector);
Suppliers/manufacturers (hardware and software);
Carriers and carrier associations;
Academia;
Consultants;
Public sector; and
Others.

Submissions not obviously from a representative of an identifiable group, were entered as individual submissions.

Analysis of responses

Part 1: Summary of quantitative results

Overall position towards controls on cryptography

From the responses to the three specific policy options presented, it was possible to get an overall indication of how cryptography controls as a whole are viewed by the respondents from the standpoint of whether existing controls should be strengthened or lessened, or whether the status quo is preferred. The results, summarized in Table 1, indicate that 78% of respondents believe that at least some lessening of controls is justified. The 14% of respondents who believe stronger measures are justified all represent the Law Enforcement/National Security grouping. 8% of respondents indicate that, overall, the status quo is appropriate.

Respondent Group	Total Responses	More Controls	Fewer Controls	Status quo
Individual	45	0	43	2
Industry Assoc.	5	0	4	1
Law Enforcement	15	15	0	0
Privacy/Human Rights Advocates	5	0	5	0
HW/SW suppliers	12	0	11	1
Carriers & Associations	4	0	4	0
Academia	14	0	12	2
Consultants	5	0	4	1
Public Sector	0	0	0	2
Others	2	0	0	0
Total	107	15	83	9
Percentages		14%	78%	8%

Table 1: Overall position on cryptography controls

Encryption of stored data

Table 2 indicates the results of the responses to the policy options suggested for encryption of stored data.

The suggested options were: market-driven; minimum standards; and mandatory access.

Here, 52% believe that the market-driven approach is best, 29% (57% of individuals) would prefer to see no controls at all, 12% (all belonging to the Law Enforcement/National Security grouping) want mandatory access and only 6% opted for the minimum standards option. In addition, three respondents indicated that they were opposed to option three (mandatory access) but did not indicate any other preference.

Respondent Group	Total	Market	Minimum Standards	Mandatory Access	No Controls	Other Preference
Individual	51	19	2	0	29	0
Industry Assoc.	4	3	1	0	0	0
Law Enforcement	16	0	1	14	0	1*
Privacy/Human Rights Advocates	5	3	0	0	2	0
HW/SW suppliers	12	10	1	0	1	0
Carriers & Associations	5	5	0	0	0	0
Academia	14	13	1	0	0	0
Consultants	5	3	0	0	1	0
Public Sector	2	2	0	0	0	0
Others	4	3	0	0	1	0
Total	118	61	7	14	34	1
Percentages		52%	6%	12%	29%	1%

Exceptions: 3 responses indicated "not option 3"

Table 2: Encryption of Stored Data

* It was suggested that a standard form of encryption be used such that the decryption key could be made available to the authorities with judicial authorization.

Encryption of real-time communication data

Table 3 indicates the results of the responses to the policy options suggested for encryption of real-time communications data.

The suggested options were: assistance orders and selective conditions of licence (status quo); obligations on all carriers; and mandatory controls.

43% of respondents indicated that no change to current procedures (ie assistance orders and selective conditions of licence) was necessary, 25% (49% from the Individual grouping) indicated that there should be no controls whatever, 11% (all from the Law Enforcement/National Security grouping) wanted mandatory controls, 6% wanted obligations on the carriers and 5% suggested other options. Significant in the responses to this question were the 12% of respondents who explicitly objected to either mandatory controls or carrier obligations (ie respondents who declined to select one of the specified options but who indicated that options 2 and 3 were unacceptable).

Respondent Group	Total	Status Quo	Carrier Obligations	Mandatory Access	No Controls	Other Preference*
Individual	47	19.5	3.5	0	23	1
Industry Assoc.	5	4	0	0	0	0
Law Enforcement[1]	16	0	2.5	12.5	0	1
Privacy/Human Rights Advocates	5	2.5	0	0	2.5	0
HW/SW suppliers	10	7	0	0	1	1
Carriers & Associations	5	5	0	0	0	0
Academia	14	4	1	0	0	0
Consultants	4	1	0	0	1	2
Public Sector	2	2	0	0	0	0
Others	2	2	0	0	0	0
Total	110	47	7	12.5	27.5	5
Percentages		43%	6%	11%	25%	5%

Exceptions: 13 responses said "not option 3" or "not option 2 or 3"

Table 3: Real-time Communications

* Other Preference suggestions included incorporation of lawful access provisions in all public key and session key transactional applications plus support for CALEA-type legislation in Canada; non-mandatory access with three types of service - local encryption, carrier encryption, or no encryption; using a subpoena to obtain information; and rejecting the options listed without offering alternatives but without actually opposing the idea of law enforcement access.

1. Where a law enforcement response simply endorsed the resolution of the Canadian Association of Chiefs of Police (Annex A), this has been interpreted as favouring mandatory controls on the basis that the resolution calls for a mandatory key recovery regime for law enforcement access plus legislation requiring contemporaneous decryption for law enforcement access to be designed into encryption services and legislation requiring communications service manufacturers, service providers and network operators to provide law enforcement access to communications.

Note: where a response indicates that either of two options is acceptable, eg carrier obligations or mandatory access, a count of .5 has been added to each option.

Export controls

Table 4 indicates the results of the responses to the policy options suggested for export controls.

The suggested options were: relax controls; maintain existing policy; and extend controls.

Of those who responded to the question on export controls, 88% indicated they wanted to see a relaxation of the current controls (71%) or no controls at all (17%), 6% favoured the status quo and 1% (representing a single law enforcement response) specifically wanted to extend controls.

Respondent Group	Total	Relax	Status Quo	Extend	No Controls	Other Preference*
Individual	26	16	0	0	10	0
Industry Assoc.	5	4	0	0	0	1
Law Enforcement	4	0	1	1	0	2
Privacy/Human Rights Advocates	4	3	0	0	1	0
HW/SW suppliers	11	10	1	0	0	0
Carriers & Associations	4	4	0	0	0	0
Academia	12	10	1	0	0	1
Consultants	5	3	1	0	1	0
Public Sector	0	0	0	0	0	0
Others	1	1	0	0	0	0
Total	72	51	4	1	12	4
Percentage		71%	6%	1%	17%	6%

Table 4: Export Controls

* One response offered no opinion but indicated they would support a federal government decision on export controls; one said that, for their purposes, the free flow of products between Canada and the US was essential; one said we should not make changes that would put Canada out of step with the US; and one opposed any further limitations on exports and rejected the suggestion that limits might be placed on the export of products lacking key recovery.

Part 2: Review of narrative responses

General observations

The comments reflect a wide recognition of the need for strong cryptography both for business and for private use. It was noted that, in addition to electronic commerce, electronic service delivery and privacy uses, businesses need to protect themselves against industrial espionage. A number of submissions from across the spectrum expressed concern over the potential effect of policy proposals on electronic commerce and service delivery. One supplier emphasized that crypto policy must support electronic service delivery objectives, not impede them. A number of the law enforcement submissions recognized the importance of cryptography to electronic commerce but cautioned that encryption must not be allowed to shield criminal activities. The need to avoid developing a policy that was unenforceable, or that regulated only the law abiding citizen, featured in a number of responses.

Twelve of the submissions pointed out the futility of trying to impose importation or usage controls on strong cryptography which is already widely and freely available. It was broadly indicated that strong crypto will always be available to criminals, whether or not restrictions are placed on its use. The availability of non-cryptographic confidentiality techniques was another frequently-mentioned issue.

One privacy association paper listed what it considered to be a number of errors and omissions in the discussion paper. These included the risk of relying on weak encryption or systems where keys must be made available to a third party; liability issues; the infeasibility of detecting the method of encryption or even whether encryption is being used at all; the omission of any concrete evidence that the use of encryption has ever been a genuine impediment to law enforcement in any specific cases; and the omission of well known examples of improper surveillance and abuse of personal privacy.

A number of submissions remarked on the US promotion of its cryptography policy interests. Ten submissions expressed concern that Canada would simply follow the US policy directions on cryptography and indicated that this was unacceptable.

Mandatory key recovery/key escrow issues

A large number of responses spoke of the impracticality of any kind of mandatory key recovery or key escrow. Specific comments emphasizing opposition to mandatory key recovery/key escrow were included in 54 of the submissions. Of these, 26 were from individuals, five from industry associations, four from suppliers, one from a carrier/association, 14 from academia and four from other groups. Only in the law enforcement submissions was there support for additional controls to provide mandatory

access to encrypted stored data. One of the law enforcement submissions, while supporting the resolution of the Canadian Chiefs of Police, noted that mandatory access is a restrictive policy and will not work. Such controls were rejected by a large majority of respondents. Reasons advanced include the following:

- any kind of key recovery for law enforcement would create points of vulnerability and weaken the value of the encryption;
- key recovery systems are less secure, cost more and are more difficult to use;
- key recovery requirements can be evaded;
- double encryption can be used to circumvent key escrow objectives;
- non-standard algorithms can be used;
- any mandatory key recovery infrastructure will be limited in its application;
- the cost of establishing and operating a key recovery infrastructure would be high and negatively affect industry's competitiveness
- key recovery is not possible for the type of strong encryption used with smart cards.

One industry association submission noted that there was no current law to prescribe how physical data should be stored and that electronic data should not be treated differently.

Five of the submissions noted that any attempt to mandate "back door" decryption in Canadian crypto products would deter overseas buyers and disadvantage Canadian exporters.

Thirteen submissions commented on the additional points of vulnerability that would be introduced with a key escrow system system and on the danger of escrowed keys being misused.

One of the carriers urged that Canada adopt a market-driven approach to strong encryption, as mandatory key recovery would put us out of step with many of our international partners.

Another point frequently made with respect to controls in Canada was that those willing to break the law would not be deterred by a legislative requirement to use cryptography with mandatory access provisions. International terrorists and criminals have access to encryption technology in the global market place. Canadians should not be prevented from protecting themselves. Controls on domestic use are widely viewed as discriminating against the honest citizen.

Several contributions highlighted the opportunities to conceal information using non-cryptographic techniques such as steganography, communicating in obscure languages and chaffing/winnowing.

Access to stored data

It was generally acknowledged that some businesses need to provide key recovery and data back-up for their own needs but it was quite strongly indicated that this should be regarded as an internal matter for business, not something to be imposed by government. It was also repeatedly indicated that any business needs in this area should not be used as a pretext to impose access requirements for law enforcement purposes. Business responses made it clear that they currently cooperate with legally authorized access requests and will continue to do so but they don't want the government telling them how to go about their business.

A number of responses suggested relying on the fact that businesses are already required to maintain certain types of record for auditing purposes and that this should suffice.

Real-time communications data recovery

Ten of the submissions (including those of three carrier/carrier associations, three industry associations, and one law enforcement agency) referred specifically to the infeasibility of having carriers or Internet Service Providers decrypt messages that have been encrypted outside of the carrier network. All the carriers/associations and two of the industry associations indicated existing methods available to law enforcement agencies are sufficient and that no additional measures are justified.

Three carrier associations and one supplier protested that the development of an infrastructure to support rapid decryption of real-time communications data would be enormously expensive, possibly in the hundreds of millions of dollars. Two of the respondents (one carrier and one association) claimed that the capability for rapid, universal decryption would have a chilling effect on the development of electronic commerce and one of the carriers noted that this would extend to the development of new encryption technologies. The term *chilling effect* was also used by one of the Privacy Commissioners in referring to mandatory controls on the use of encryption for real time communications since "secret monitoring and surreptitious access to private keys would create the it would create the conditions for a surveillance society".

Several responses noted that carriers do not retain copies of any information that passes through the network. A requirement to retain session keys would be a tremendous burden and would likely violate the *Telecommunications Act* which requires carriers to carry their customers' traffic without interference as to form or content.

One of the carrier responses noted that criminal law has never allowed officials to monitor *all* criminal communications or to seize *all* relevant criminal information.

It was also noted that, while businesses may have their own requirements for key recovery in the case of stored data, they seldom if ever have such a requirement in the case of real-time communications.

Cost issues

It is generally recognized in the submissions that any form of mandatory access provision, key recovery infrastructure or enhanced law enforcement access provisions will be very expensive. In all, 21 responses, including some from law enforcement agencies, observed on the high cost and several, including two carriers/associations, noted that the cost to business of regulated key recovery will make Canada uncompetitive internationally.

Opinions are offered by all groups on the issue of who should pay these costs. These positions can be collectively summarized in the two words "not us". Some of the law enforcement responses suggested that the carriers, suppliers or subscribers should bear the costs while some of the individual, corporate and carrier/association responses suggested that those who require the service (ie the government/law enforcement agencies) should pay.

Other cost issues were raised in the context of whether the government had done its homework in evaluating the costs, benefits and other implications of the crypto policy proposals. For instance it was noted that the differences between commercial and military/security uses of encryption have not been sufficiently defined and that cost and ease of use are not primary considerations in military/security environments as they are in commercial environments. One industry association submission urged the government not to proceed with cryptography policies or laws until an independent review has been completed to determine the cost, benefit, and risks of proposed options.

One industry association raised the issue of the costs involved in interfacing the private sector and institutional Public Key Infrastructures (PKI) to the Government of Canada PKI and recommended the costs be "reasonable, transparent and applied in a uniform manner to all PKIs, both private and governmental".

Privacy issues

Seventy-two submissions (39 from individuals, 16 from academia, 5 from privacy and human rights interests, 4 from suppliers, 3 from carriers/associations, 3 from the public sector and 2 from others) contained comments on the likely adverse impact of the policy proposals on the individual. This single issue drew more specific comments than any other. The issue of greatest concern was that law-abiding citizens would be disadvantaged by proposals to support law enforcement needs. One carrier association noted " legitimate law enforcement concerns should not be dealt with in a manner which effectively limits private citizens' legitimate use of encryption or reduces the benefits that will accrue to the private sector by

the use of strong encryption." A carrier observed that "any limits on crypto must be demonstrably justifiable in a free and democratic society" and that "measures to prohibit the use of non-accessible encryption products infringe on Canadians' right to chose and use measures they consider appropriate to safeguard their own security." Another carrier association stated that "the concerns of law enforcement agencies should not be accommodated in a manner that effectively limits legitimate private use of encryption".

A letter signed by 20 international human rights groups itemized the reasons for opposition to the policy proposals, claiming that, in their collective opinion, such policy or legislation would be "contrary to international human rights treaties, harmful to Canadian society, detrimental to the Canadian economy and in the end, simply unenforceable."

A number of submissions emphasized the distinction between confidentiality, as needed in business-to-business transactions and privacy as needed in transactions between clients and service providers, privacy being a relationship issue rather than a confidentiality issue. One individual response recommended that the right to privacy should not imply a right to anonymity and suggested that there should be no right to anonymity for mass e-mailers or those posting web pages on business or public matters.

Law enforcement issues

It will be noted from the quantitative responses that there appears to be a strong division of opinion between the law enforcement/national security interests and the rest of the respondents on the issue of control of cryptography. This is in part due to the fact that many of the law enforcement responses simply endorsed, without qualification, the August '97 resolution of the Canadian Association of Chiefs of Police(Annex A) which proposes, inter alia, establishment a mandatory key recovery regime and legislation requiring real-time decryption for law enforcement access purposes. The parts of this resolution that propose mandatory, or additional controls on encryption have been strongly rejected by the vast majority of other respondents. On the other hand, some of the law enforcement responses reflect a recognition of both the challenges presented by cryptography and the need to find an acceptable solution that meets law enforcement needs without violating the rights of the individual. One law enforcement submission noted that, while the demands may appear to be an obstacle to progress, law enforcement is not looking for increased investigative capabilities or new authorities, merely to restore and maintain what was available before.

Overall, the submissions strongly support the statement made by one respondent that there is no popular consensus, outside the law enforcement community, that regulation of cryptography is needed. Forty-six submissions provided comments indicating that they believe no regulation of cryptography is needed and/or that existing methods available to law enforcement agencies to obtain information are sufficient to protect public safety and national security. These responses included 28 from individuals, 5 from carriers/associations, 5 from

privacy interests, 2 from industry associations and 6 from other groups. One carrier association noted that "the needs of users, carriers and third-party suppliers of E-commerce are in some cases in direct conflict with the stated needs of law enforcement and security agencies". A number of submissions, including one from a Privacy Commissioner, observed that the law enforcement agencies have not proven that the interception and decryption capabilities sought will lead to a decrease in criminal activities and it was clearly indicated that many respondents (46 submissions) believe that existing methods available to law enforcement agencies to obtain information are sufficient to continue to protect public safety and national security.

Although many of the submissions recognized the need to find a solution to the problems posed for law enforcement by strong cryptography, the impracticality of trying to control cryptography was repeatedly emphasized and there was virtually no support for mandatory key recovery or mandatory controls on carriers beyond the measures that currently exist.

While some of the demands made in the law enforcement submissions appear unlikely to find much support in the community at large (eg the requirement for registration of every Canadian citizen and landed immigrant in a key recovery system and the assignment of a unique password to all registrants) other police agency suggestions are more in tune with the bulk of submissions in that they recognize the technical difficulty, impracticality and cost implications of trying to apply mandatory access controls for stored data or mandatory access requirements on the carriers. Implicit in a small number of the law enforcement submissions is a recognition that the problem faced by law enforcement is not one of cryptography alone, but of the rapid pace of technological change and development of technical capabilities that can be abused. Comments that law enforcement agencies are not equipped to deal with current technology appeared in several contributions including a number from the law enforcement agencies themselves. It was suggested that additional tools, technical information, technical support, more resources to monitor and detect breaches, plus a national strategy are needed to keep abreast of the technology and to help technology fulfil the promise of aiding, rather than hindering, law enforcement.

Several proposals to meet law enforcement needs were made by groups other than the law enforcement agencies. These include: using court orders to gain access to keys; enforcing existing laws on surrender of information; gathering information by means other than examining encrypted files; cryptanalysis; and using existing and emerging techniques for gathering computer and non-computer data. One law enforcement submission recommended, as an alternative to mandatory controls, minimum standards to allow the federal government to provide education, direction and structure for cryptographic use and development. Another law enforcement response, recognizing the magnitude of the task of trying to apply encryption regulations, recommended that, "if the problem defeats all attempts at legislative control, alternative strategies and support for the development of investigative techniques be

pursued in parallel with existing initiatives". One industry association suggested the need for on-going dialogue between encryption producers, users and law enforcement agencies and offered to host such a dialogue.

The recommendation that use of cryptography in the commission of a crime be criminalized is included in the resolution of the Canadian Association of Police Chiefs and is frequently mentioned in the submissions from the law enforcement community. While there is no indication of strong support for this from the other submissions, it was also suggested by one of the industry associations.

Export Controls

Two issues come through very strongly here: Canada is being placed at a competitive disadvantage by the current application of export controls; and it is necessary to work in concert with the international community.

From the quantitative results, it can be seen that only 7% of respondents favour maintaining the status quo or extending export controls. In every group of respondents other than the law enforcement group, the majority favoured relaxation of controls. (Only four of the law enforcement submissions responded on the export control issue. One favoured extending controls, one favoured the status quo, one opted to remain neutral on the subject but to support any federal government initiative or decision, and one acknowledged there are some arguments in favour of relaxation but urged caution and noted the need to remain aligned with the US.)

Twenty-four submissions (including those of three industry associations, four carrier/associations and eight suppliers) included comments on the negative effects of current restrictions on the export of cryptography. The point that export controls put Canadian cryptography suppliers and producers at a competitive disadvantage was particularly emphasized. Many of those arguing for relaxation of export controls also emphasized the need to continue to work with the international community on this issue but, as several submissions observed, the Wassenaar provisions are being flexibly interpreted by some other countries. The example of the US giving blanket approvals to certain companies to export strong cryptography was given in considerable detail in one of the submissions. Germany, Switzerland and the Republic of Ireland were also mentioned as countries that allow companies to freely export cryptography products. It was noted that Canada fails to take advantage of this flexibility within the Wassenaar arrangement.

Although there is an overall clear preference for export controls to be eliminated, it was strongly suggested that, if export controls are to remain in effect, Canada should take maximum advantage of the flexibility under the Wassenaar arrangement to liberalize the controls to the greatest extent possible.

Two of the submissions argued that commercial crypto products should not be

subject to military technology controls noting that crypto products are important commercial tools and are now used more by business than by the military.

Suggested options for the export rules include giving blanket export approval for encryption up to a certain key length with case-by-case approvals for key lengths greater than that specified (128 bit keys for symmetric and 1024 bit keys for asymmetric encryption are recommended). Another suggestion is that export controls be abandoned except for specific embargos to individual countries. It is also suggested that both public domain and mass market software and hardware should be exempt from controls, that general approval be given to export a product, rather requiring individual licences for each export instance, and that Canadian exporters be permitted to match the product exports of other countries with products of similar strength.

The need for suppliers and carriers to be treated equally

Although mandatory controls and regulations are generally opposed, the point is frequently made that, any policy decisions must be technology-neutral and, if there are to be obligations placed upon suppliers, there must equal treatment for all.

In particular, three carriers/carrier associations urged that the application of assistance orders and obligations to cooperate with law enforcement agencies should apply to all carriers and service providers, not just those considered to be part of the public switched telephone service. One of the law enforcement submissions also noted the need for equal treatment for industry in the application of mandatory access and lawful interception. One submission commented that selective controls and licencing (such as licencing conditions imposed on wireless carriers) distort the market place and place an unfair burden on particular suppliers. As one submission observed: "As the telecommunications industry is becoming increasingly competitive, it would be inappropriate for the government to create a policy that distributes the burden of complying with policy directives in a manner that creates a competitive disadvantage for one type of service provider over another."

The carrier associations and two suppliers also recommended that any controls placed on the commercial use of encipherment should apply to all sectors of the economy.

The issue of equal treatment also came up with respect to export restrictions where one supplier urged that mass market and generally-available crypto hardware be given the same treatment as crypto software.

Legislation, regulation and Charter issues

Nineteen submissions (14 from academia, two from carriers/associations, two from privacy interests and one from a privacy commissioner) expressed concern that policy proposals for law enforcement and mandatory controls on real-time communications would violate the *Charter of Rights and Freedoms*, and/or laws including the *Telecommunications*

Act. Some of the law enforcement submissions noted that any potential legislation must be

in accordance with the *Charter of Rights and Freedoms*. One of the law enforcement submissions suggested that arguments presented as to the *Charter* rights of Canadians to enjoy privacy and freedom of expression should be a "none issue" (sic) as any interception would require justification and the prior approval of the courts.

Liability issues were raised in five of the contributions, particularly the liability of third parties for the unauthorized release of confidential information, such as keys, and the liability issues that arise if companies are required to keep confidential information but are constrained by law to use only weak encryption or encryption with third party access.

One of the law enforcement responses noted that there is no specific authority in the *Criminal Code* that compels the possessor of a cryptographic key or a password to divulge the information. It was also noted in the same submission that recent *Criminal Code* amendments react to problems after they occur, which makes it difficult for law enforcement agencies to stay ahead of the technology.

A number of submissions urged that any action by the government should be proportionate to the extent and significance of the problem, and that account be taken of the probable cost of the response and the likely effect on both the targeted population (eg criminals) and everyone else (business and commerce, service providers, equipment and software providers, and users and the public at large). A number of individual and privacy/human rights submissions questioned the need to limit the privacy rights of all Canadians on the basis of assumptions and suppositions, devised by law enforcement and national security interests, when there is no real evidence that police investigations are being critically impaired by cryptography. An industry association pointed out any law enforcement and national security requirements that limit the application of strong cryptography would not only compromise the industry's security programs but might also have associated costs that offset the consumer benefits of electronic commerce. A number of submissions urged that a full cost benefit analysis be conducted before taking decisions on any proposals. Others recommended avoiding setting up a decryption/monitoring facility for all users when only a small number are targeted.

Submissions from the public sector/Privacy Commissioners stressed the need to ensure that the required encryption infrastructure is secure and trusted and also that cryptography policy binds trusted third parties to strict privacy principles and practices.

Other issues

A number of submissions pointed out that a strong case can be made that widespread use of strong encryption may advance effective law enforcement more than it may permit some individuals and organization to communicate privately about illegal acts.

Six submissions urged that cryptography policy and rules take full account of open, international standards. One industry association response referred to the patchwork of digital signature legislation in the US and said that standards are needed in Canada to avoid the same thing happening here.

One association pointed out the need for caution in using imported crypto products which could have undocumented features that allow third parties surreptitious access to a user's transactions. Some form of assessment and certification of crypto products was suggested.

A corporate submission urged that companies with a large customer base should be allowed to provide Certificate Authority services.

Conclusions and possible follow-on actions

A number of strong messages emerge from the comments and responses. It is clearly indicated by the majority of responses and the accompanying rationale that:

- mandatory controls on the use or importation of encryption facilities are unacceptable to business, industry, commerce, privacy and human rights advocates, academics and private individuals, as is any kind of mandatory key escrow/key recovery system;

- mandated access to decrypted real-time communications data can only be achieved at great cost and at significant risk to Canadian competitiveness and personal privacy;

- new measures to provide access to encrypted stored data are generally regarded as unjustified and unnecessary;

- current application of export controls is inconsistent internationally and is disadvantaging Canadian business;

- market-driven solutions are preferred to other alternatives for the listed policy options;

- law enforcement agencies face a significant challenge to some of their traditional investigative techniques from strong cryptography and other technological developments.

- there is serious concern that actions stemming from current policy proposals will have an adverse impact on personal privacy, and in particular, that law-abiding citizens will be disadvantaged by proposals to support law enforcement needs.

The following is a summary of possible actions suggested by the submissions to meet the needs of law enforcement agencies, business, industry, commerce, and the private citizen:

- federal legislation to make it an offence to use encryption to conceal criminal activity;

- changes to the *Criminal Code* to make it an offence to refuse to surrender an encryption key or to provide plaintext information in response to a court order;

- federal legislation to legitimize and recognize the use of digital signatures;

- federal legislation to protect the cryptography user against unauthorized release of his/her key, or other protected information, by third parties;

- assistance to the law enforcement agencies to enable them to keep abreast of technological change and to use the technology in a practical and realistic way to assist them in upholding the law;

- establishment of an on-going dialogue between law enforcement agencies, service providers, and cryptography and other hardware and software suppliers to assist law enforcement agencies in their task;

- progressive easing of export restrictions, consistent with Canada's Wassenaar obligations

- active encouragement of the legitimate use of strong cryptography as a way of building confidence in secure electronic commerce and electronic service delivery and as a way of reducing electronic crime.

Part 3: Suggestions for expediting the rollout of secure electronic commerce

Responses to the invitation to comment on measures to accelerate the rollout of secure electronic commerce were contained in a number of the submissions, though many of the respondents chose to confine their remarks to the cryptography policy issues. The suggestions below are drawn from the submissions that elected to comment on this issue.

Legal issues

1. Establish legislation that is formulated to provide a national framework that recognizes the validity of electronic authentication methods with the same standing as written signatures.

2. In facilitating the admissibility of computer-generated records for evidentiary purposes, ensure that laws facilitate the use of electronic methods (such as digital signatures), rather than imposing onerous and complicated regulatory schemes as has been done in some jurisdictions.

3. Foster an environment in which the market place, through national and international standardization schemes, is encouraged to develop the detailed procedures to underpin the reliability of authentication schemes.

4. Work to clarify the liability rules, particularly those associated with digital signatures and the unauthorized release of information by third parties.

Trusted Third Parties

1. Adopt a market-oriented approach to the establishment of Certification Authority services. A licencing regime at this point would be a burden on both the electronic commerce users and the emerging infrastructure. (Note that some existing institutions, such as the financial institutions, the Passport Office and the Post Office, appear well qualified to act as CAs.)

2. Recognize that the best way to achieve effective business practices for CAs, with minimum impact on cost and efficiency, is to encourage the private sector to develop CA procedures, in consultation with the public sector.

Lead by example

1. The government should play a leadership role as a model user of electronic commerce and electronic service delivery and also play a major role in the public promotion of these services and in educating consumers in their use.

2. The federal government should expand upon its role as a model Internet user and purveyer of on-line services, such as electronic tax filing, by accelerating and expanding the range of on-line services (for example electronic forms are not yet available via the Internet) and by enabling the citizen to interact directly with departments.

Security for electronic commerce

1. Recognize that cryptography is only one component in the security infrastructure that is essential for on-line government services. It is essential that information stored locally be securely held, be safe from intrusion and be recoverable in the event of failure or disaster.

2. The application of cryptographic products and services will have an enabling effect on all

sectors of economic and social activity. Without wide availability and deployment of encryption, the ability to create new, more competitive forms of business will be substantially inhibited. Strong cryptography is necessary to the success of electronic commerce and its use should be encouraged.

3. Ensure that any policies are based on open, international standards.

4. Ensure that protocols, software and encryption algorithms are well documented and freely available so that knowledgeable users can verify the strength and quality themselves. Avoid restrictions on the design, creation or implementation of strong cryptography.

5. Consider establishing, or recognizing, an independent assessment facility to provide users with assurance of the strength and reliability of cryptographic algorithms.

Role of government in promoting the electronic services

1. Consumers do not yet feel confident that the Internet is a safe way to transact business. The government needs to work with the private sector to develop effective security procedures and to educate the public about those procedures. Work to build consumer confidence.

2. Avoid over regulation, which will stifle technological development and hamper consumer confidence in electronic commerce.

3. Ensure that policies on cryptography do not unduly interfere with the ability of Canadians to protect the privacy and integrity of their electronic communications.

4. Avoid any measures that would unduly increase the cost of doing business electronically.

5. Support and actively assist the Canadian IT industry in providing security for electronic commerce.

6. Acquire and promote Canadian IT security products and services.

7. Encourage inter-operation of federal government security infrastructures (such as PKI) with the other public and private sector security infrastructures.

8. Allow the market place to work and ensure a level playing field for the Canadian IT security industry.

9. Work towards ensuring that everyone has access to on-line services, not just those who can afford their own computers and Internet services.

10. Avoid forcing people to purchase specific commercial software, or to go through

particular agents, as is now required for electronic tax filing.

11. Ensure costs of inter-operating with the government security infrastructures is low.

International issues

1. Continue to work in international fora to promote secure global electronic commerce and reduce barriers to global trade in cryptography products and services.

Closing remarks

The analysis provided in this report is, of necessity, limited to an overview of the most frequently occurring issues together with a subjective selection of some of the less frequently identified concerns. Although such analysis can provide an overview of the broad consensus, the richness of detail and the particular insights reflected in the individual responses cannot be captured except to a very limited extent. As mentioned earlier in this report, the individual submissions reflect a great deal of thought and effort on the part of the individuals and organizations who responded to the Industry Canada paper. These contributions provide a wealth of detail and much insight into the difficult task of developing a balanced Canadian policy on cryptography. Thanks are due to everyone who took the trouble to respond on this topic and who has in some way contributed to developing a consensus on this topic.

Annex A: Resolution of the Association of Canadian Chiefs of Police, August 1997

Therefore be it resolved that the Canadian Association of Chiefs of Police urges that the Government of Canada:

1. Establish a Public Key Infrastructure requiring licenced Certification Authorities and a mandatory key recovery regime which will provide for lawful access to cryptographic keys;

2. Enact appropriate legislation, including Criminal Code amendments to make the use of encryption in the commission of a any crime an offence and permitting the seizure of any equipment utilized for the purposes of encryption;

3. Enact appropriate legislation requiring that hte providers of encryption services to design such services to permit contemporaneous or real-time decryption for the purposes of lawful access by law enforcement and national security agencies;

4. Enact appropriate legislation to ensure that existing or emerging communications services manufacturers, services providers and network operators provide lawful access to communications at no cost to law enforcement agencies;

5. Establish an appropriate legislative and policy base to allow the Communications Security Establishment (CSE) to provide assistance to Canadian law enforcement and national security agencies in the area of cryptography and similar technology used in the commission of an offence;

6. Establish government standards to ensure confidence in information infrastructure which would reduce the potential of their use for criminal enterprise or other uses which are contrary to the public interest;

7. Increase the availability of resources to permit a higher level of research and development of technological and other measures to remove some of the obstacles to law enforcement and national security posed by cryptography and similar technology.

Annex B: Index of Submissions to the Discussion Paper

1) Summaries of Submissions from Organizations

Action Software International	042
Alliance of Manufacturers & Exporters Canada	1-314
Brockville Police	070
British Columbia Civil Liberties Association	139
Canada Post (Electronic Services)	1-302
Canada Post (Electronic Products and Services)	1-308
Canadian Advanced Technology Assoication (CATA)	125
Canadian Association of Internet Providers	123
Canadian Bankers Association (CBA)	118
Canadain Business Telecommunications Alliance (CBTA)	1-317
Canadian Cable Television Association (CCTA)	112
Canadian Security Intelligence Service	1-311
Canadian Wireless Telecommunications Association (CWTA)	166
Chrysalis-ITS	129
City of Charlettetwon Police Headquarters	063
Commission d'accès à l'information du Quebec	094
Delta Police Department	160
DMR Consulting Group Inc.	037
Domus Software	126
EWA	168

Edmonton Police Service	171
Electronic Frontier	116
Entrust Technologies	130
Gandalf Graphics Limited	157
GT Group Telecom Inc.	031
H&R Block Canada Ltd. (Calgary)	163
Halifax Regional Municipality	169
Hewlett-Packard (Canada)Ltd. (Mississauga)	137
Information and Privacy Commissioner/Ontario (Ann Cavoukian)	128
Information Systems Manager Hyprotech Ltd. (Calgary)	156
Information Technology Association of Canada	153
Information Technology Laboratory National Institute of Standards and Technology	006
Institute for the Study of Privacy Issues (ISPI)	090
Intelligent Switched Systems	077
IT Management Consultant	013
KPMG	133
La Fédération nationale des associations de consommateurs du Québec et Option consommateurs	143
London Police	093
Manitoba Association for Access and Privacy	124
Metropolitan Toronto Police	142
Microcell Telecom Munications Inc.	136

Mimosa Systems Inc.	146
MIT Lab for Computer Science	046
Motorola Canada Limited	141
Northern Lights College	045
Okiok Data Ltd.	099
Prince Albert Police Service	170
Privacy Commissioner of Canada	162
Queens University	101
Regina Police Service	167
Rogers Communications Inc.	152
Science, Research and Information Technology (Alberta)	127
Royal Canadian Mounted Police (Ottawa)	095
Royal Canadian Mounted Police (Ottawa)	097
Royal Canadian Mounted Police (Vanier, Ont.)	1-312
Royal Canadian Mounted Policy (Victoria, BC)	164
Royal Canadian Mounted Police (Whitehorse, Yukon)	115
Royal Newfoundland Constabulary	092
Stentor Telecom Policy Inc.	131
Telus Corporation	140
The London School of Economics and Political Science	135
Timestep Corporation	087
Twiggy Design	113
Université de Montréal	144

University of Toronto	039
University of Toronto (Department of Electrial and Computer Engineering)	138
Valmet Automation	108
Vancouver Webpages	081
Vidéotron Télécom ltée	1-318
Victoria Police Department	117
Ville de Québec Servic de police	159
Windsor Police Service	067
WinMagic Inc.	098
Winnipeg Police Service	047

2) Summaries of Submissions from Individuals

Arzumania, Ara	066
Bartel, Mark	056
Bernier, M.V.	058
Caldwell, Joshua	1-310
Chappel, David A.	1-313
Chin, Tony	052
Clayton, Michael J.	079
de Raadt, Theo	002
Darwin, Ian	132
Décarie, Richard	102
Duford, Lee	059

Galloway, Dave	154
Graham, Hugh	121
Gregory, Don W.	091
Harminc, Tony	1-300
Hart, Rob	085
Hayes, Amos	1-301
Hekimian, Hrad	066
Hinke, C.J.	1-315
James, Mark	100
Jeffery, Jim	027
Jeppsson, Jonas	119
Klassen, Arthur N.	078
Kossmann, William	054
Litwyn, Jay	015
Lloyde, William	032
Lynne, Stuart	053
MacGregor, John	060
Macrae, Robin	1-309
Maniscalco, Nick	109
Martin, C.	062
McCutcheon, Mark	151
McElvanney, Matthew	034
Milliken, Peter (House of Commons, Kingston)	172

Narveson, Jan	106
O'Malley, Sarah	155
Perrin, D.B.	040
Pick, Jim	089
Plumb, Marc	107
Quinton, Reg	075
Reid, Robert	103
Robinson, Ken	145
Sampson, Curt	076
Savard, John	104
Schuetz, Marko	110
Smith, Eric S.	1-316
Spencer, Henry	158
Streifling, Jeffrey	073
Tarrant, Keith	035
Tomlin, Gord	042
Taylor, M.	1-303
Tyler, Nicholas	064
Tyson, Al	033
Wilson, Brad	072

Document de travail sur la politique en matière de cryptographie : analyse des observations reçues

Préparé par

AEPOS Technologies Corporation

PRÉPARÉ POUR : Industrie Canada

AUTEUR : AEPOS Technologies Corporation
116, rue Albert, bureau 601
Ottawa (Ontario)
K1P 5G3

DATE : 11 juin 1998

Le présent document est également diffusé en version électronique sur le Web à :
http://strategis.ic.gc.ca/crypto

Il est aussi offert sur demande dans une présentation adaptée à des besoins particuliers. Communiquez avec les personnes dont les coordonnées figurent ci-dessous.

Pour obtenir des exemplaires du présent document, veuillez vous adresser à :

Donna Emmett
Groupe de travail sur le commerce électronique
Industrie Canada
300, rue Slater, bureau 2022A
Ottawa (Ontario)
K1A 0C8

Tél. : (613) 990-9233
Téléc. : (613) 941-0178
Courrier électronique : emmett.donna@ic.gc.ca

Vous pouvez contacter Michael Harrop à :

AEPOS Technologies Corporation
116, rue Albert, bureau 601
Ottawa (Ontario)
K1P 5G3

Tél. : (613) 599-5905
Téléc. : (613) 599-4681
Courrier électronique : mharrop@bigfoot.com

© Sa Majesté la Reine du chef du Canada (Industrie Canada) 1998
N° de catalogue C2-336/2-1998
ISBN 0-662-63949-9

Table des matières

Introduction 1

Observations générales à propos des commentaires reçus et du processus d'analyse 3

Analyse des réponses 5
- Partie 1 : Résumé des résultats quantitatifs 5
  - Position d'ensemble à l'égard des contrôles en matière de cryptographie ... 5
  - Chiffrement des données stockées 6
  - Chiffrement des communications en temps réel 7
  - Contrôle des exportations 9
- Partie 2 : Examen des réponses narratives 10
  - Observations générales 10
  - Récupération obligatoire des clés et problèmes relatifs à l'entiercement des clés 11
  - Accès aux données stockées 12
  - Récupération des données de télécommunications en temps réel 12
  - Questions de coût 13
  - Questions relatives à la protection des renseignements personnels 14
  - Questions relatives à l'application de la loi 15
  - Contrôle des exportations 17
  - Nécessité de traiter les fournisseurs et les entreprises de télécommunications sur un pied d'égalité 19
  - Questions relatives à la législation, à la réglementation et à la Charte des droits 19
  - Autres questions 21
  - Conclusions et mesures de suivi possibles 21
- Partie 3 : Suggestions en vue d'accélérer le déploiement du commerce électronique sécuritaire 24
  - Problèmes juridiques 24
  - Tiers de confiance 24
  - Prédication par l'exemple 25
  - Sécurité du commerce électronique 25
  - Rôle de l'État dans la promotion des services électroniques 25
  - Enjeux internationaux 26

Remarques finales 27

Annexe A : Résolution de l'Association canadienne des chefs de police, août 1997 .. 28

Annex B : List des mémoires reçus en réponse au document de travail 29

Introduction

Le présent rapport contient une analyse des réactions au document de travail d'Industrie Canada intitulé *Politique cadre en matière de cryptographie aux fins du commerce électronique* (février 1998). Ce document a été publié le 21 février 1998, la date limite pour la réception des commentaires ayant été fixée au 21 avril suivant. Au total, le Ministère a reçu 189 réponses avant cette date et 15 autres réponses lui sont parvenues entre la date limite et le 22 mai.

En plus des commentaires en réaction au document de travail, les réponses comprenaient des demandes de renseignements additionnels, des messages électroniques et des lettres accusant réception du document de travail, de la publicité par courrier électronique (polluriel), des messages qui semblaient n'avoir aucun rapport avec le sujet (tels qu'une demande d'aide concernant un problème de consommation), des doubles de mémoires présentés au moyen de divers mécanismes de livraison et à divers moments ainsi que des télécopies de caricatures. Ces réponses n'ont pas été incluses dans l'évaluation quantitative de l'analyse.

L'analyse statistique ne tient pas compte des contributions reçues en retard, mais les commentaires ont été pris en considération dans le processus d'évaluation.

Le nombre total d'observations reçues s'établit comme suit :

Nombre total de réponses reçues à temps :	189
Réponses non analysées (voir ci-dessus) :	53
Observations reçues à temps et analysées :	136
Observations reçues en retard :	15

Nombre total de réponses (en date du 22 mai 1998) : 204

Les observations reçues représentent un large échantillon d'intérêts. Outre les 77 réponses envoyées par des particuliers et des universitaires, le Ministère a reçu des observations de 13 fournisseurs ou fabricants, de 18 organismes d'application de la loi des quatre coins du pays, de 4 organismes du secteur public (notamment de 3 bureaux de commissaires à l'information et à la protection de la vie privée), de 5 associations industrielles, de 5 organismes de protection de la vie privée ou de défense des droits de la personne, de 5 entreprises de télécommunications ou associations de télécommunicateurs, de 5 consultants et de 4 autres organisations. Les associations de télécommunicateurs représentaient toutes les compagnies de téléphone provinciales ainsi que quelques sociétés de communications sans fil. Les associations industrielles comprenaient des représentants des institutions financières canadiennes de tout le pays, 110 fournisseurs de services Internet, plus de 3 500 manufacturiers et sociétés exportatrices, les intérêts des utilisateurs de télécommunications de plus de 400 entreprises, gouvernements et fournisseurs de services de

santé qui, tous ensemble, comptent plus de 2 millions d'employés, et plus de 1 300 entreprises du secteur de l'informatique (matériel, logiciels et services) dont le chiffre d'affaires dépasse les 45 milliards de dollars et qui emploient au-delà de 290 000 personnes.

Un certain nombre d'observations sont arrivées indirectement. C'est le cas de 14 lettres individuelles qui étaient adressées à Industrie Canada comme réponses mais qui accompagnaient les observations de La Frontière Électronique du Canada; c'est également le cas de quelques observations venant d'organismes d'application de la loi, lesquelles avaient été adressées à la GRC, au Service de police régional d'Ottawa-Carleton et au Solliciteur général de l'Ontario plutôt qu'à Industrie Canada. Chacune de ces contributions a été incluse comme une observation distincte. De plus, une lettre commune signée par 20 organisations internationales qui s'occupent de la défense des libertés civiles et des droits de la personne sur Internet accompagnait le mémoire de La Frontière Électronique du Canada. Pour les fins de l'analyse, cette lettre a été considérée comme faisant partie du mémoire de La Frontière Électronique du Canada et non comme une contribution distincte.

Les observations étaient de longueur variable et leur degré de précision variait également, depuis les très brefs messages électroniques protestant contre toute forme de contrôle de la part de l'État jusqu'aux mémoires très copieux, en bonne et due forme, préparés par des comités. Toutes les réponses qui ont été considérées comme ayant rapport au sujet ont été incluses dans l'analyse, peu importe leur origine, leur teneur ou leur degré de précision.

Huit des contributions, notamment celle d'une association de télécommunicateurs, expriment leur inquiétude et leur désappointement du fait que le document de travail semble avoir un parti pris pour la satisfaction des besoins des organismes d'application de la loi en ce qui concerne l'accès à l'information électronique. Des intervenants suggèrent que l'on insiste davantage sur les aspects positifs de la cryptographie et sur la protection des droits individuels au lieu d'imposer des restrictions aux particuliers et aux entreprises. Plusieurs commentaires portent également sur l'utilisation de l'expression *accès légitime* dans le document de travail; suivant leurs auteurs, il s'agit d'un euphémisme pour désigner l'accès par les organismes d'application de la loi, étant donné que tous les systèmes de cryptographie permettent aux utilisateurs légitimes d'avoir légitimement accès aux données.

Un certain nombre d'intervenants remercient Industrie Canada d'avoir présenté les enjeux dans un document de travail public et de leur avoir donné l'occasion de participer au débat. L'ampleur du document de travail fait souvent l'objet d'éloges. Certains intervenants fournissent des éclaircissements et des corrections ou donnent des détails; d'autres protestent contre la brièveté de la période d'examen. Dans l'ensemble, les commentaires au sujet du document de travail et du processus sont plutôt favorables, la plupart des intervenants se montrant satisfaits d'avoir eu l'occasion de participer au processus d'élaboration de la politique.

Observations générales à propos des commentaires reçus et du processus d'analyse

Avant de passer à l'analyse des réponses à chacune des questions, il est de mise de dire quelques mots de l'approche générale et du processus employé pour l'évaluation des commentaires.

Comme nous l'avons indiqué précédemment, les réponses varient considérablement par leur ampleur et leur degré de précision. Certaines réponses ont été envoyées par des particuliers; d'autres, par des entreprises ou des organismes du secteur public; d'autres sont venues de groupes d'intérêts et d'associations; d'autres, enfin, proviennent d'associations industrielles. Certaines réponses traitent directement des questions abordées dans le document de travail et offrent des réponses aux questions soulevées alors que d'autres font davantage la synthèse des questions de fond. Quelques réponses couvrent une large gamme de sujets alors que d'autres ne portent que sur une seule question ou sur une sous-série de questions soulevées dans le document. Certaines observations sont très directes et vont droit au but; d'autres, par contre, fournissement des réponses qui sont parfois lourdement masquées par les commentaires qui les accompagnent. Dans l'ensemble, cependant, on voit que les intervenants ont beaucoup réfléchi et qu'ils ont fait des efforts considérables; leurs réponses permettent de bien comprendre les questions faisant l'objet de la discussion et elles présentent l'opinion réfléchie d'un vaste public. Si l'analyse présentée ici permet d'offrir une vue d'ensemble des réflexions et opinions collectives, les observations prises individuellement doivent quand même être considérées comme la réponse première au document de travail.

L'analyse présentée dans ce rapport est en partie quantitative, en partie qualitative. La majeure partie des observations reçues comprend des réponses narratives à des questions relativement ouvertes. Il n'y a malheureusement pas de moyen fiable ou reconnu pour évaluer quantitativement les réponses à des questions ouvertes. Même les réponses à des questions relativement fermées (comme c'est le cas des options en matière de politique suggérées à propos de la manière d'aborder le chiffrement des données stockées et des communications en temps réel et le contrôle des exportations) ont souvent tendance à être des réponses ouvertes plutôt que le simple choix de l'une des options. Ainsi, même avec des réponses fermées, il a souvent été nécessaire d'interpréter une réponse narrative comme indiquant une des options proposées (ou peut-être comme n'en indiquant aucune). Les intervenants qui ont répondu « pas l'option 2 ni l'option 3 » au lieu de manifester simplement une préférence pour l'option 1 présentent encore un autre problème. Dans l'ensemble, la méthode employée pour évaluer les réponses aux questions fermées consistait à réunir les réponses par groupes d'intervenants en fonction de chacune des rubriques. Lorsque aucune option préférée n'était indiquée ou lorsque l'intervenant n'avait pas fait de commentaire sur la question, on n'a pas tenu compte de sa contribution pour cette question en particulier. (Ce ne sont pas tous les intervenants qui ont répondu à toutes les questions.) L'évaluation des réponses fournies aux questions fermées qui en résulte devrait, croit-on, constituer une évaluation quantitative raisonnablement exacte.

La présentation de l'information qualitative est beaucoup plus difficile, étant donné qu'elle comporte inévitablement un certain degré de subjectivité. La méthode choisie a consisté à chercher les points abordés le plus souvent et à présenter un résumé des problèmes mis en lumière. De plus, et ce qui est le plus subjectif de tout, nous avons inclus des points qui semblent avoir une certaine pertinence pour le débat ou qui pourraient présenter des idées nouvelles, même s'ils n'ont peut-être pas été mentionnés fréquemment.

Les résultats qualitatifs ont de la valeur aussi bien que les résultats quantitatifs, mais chaque type de résultat fournit un éclairage différent. Les résultats quantitatifs peuvent donner une image d'ensemble des préférences déclarées; quant aux résultats qualitatifs qui se trouvent dans les réponses narratives, ils présentent les justifications sous-jacentes aux préférences déclarées et ils exposent aussi les incidences qui découleront vraisemblablement de l'adoption de telle ou telle orientation.

Finalement, pour les fins de l'analyse, nous avons réparti les réponses suivant les catégories ci-dessous :

Particuliers;
Associations industrielles;
Application de la loi et sécurité nationale;
Groupes de défense de la protection de la vie privée et des droits de la personne (à l'exclusion des organismes gouvernementaux);
Fournisseurs/fabricants (matériel et logiciels);
Entreprises de télécommunications et associations de télécommunicateurs;
Universitaires;
Consultants;
Secteur public;
Autres.

Les observations qui n'étaient manifestement pas celles d'un représentant d'un groupe identifiable ont été considérées comme des observations venant de particuliers.

Analyse des réponses

Partie 1 : Résumé des résultats quantitatifs

Position d'ensemble à l'égard des contrôles en matière de cryptographie

À partir des réponses aux trois options précises en matière de politique qui ont été présentées, il est possible de dégager une indication générale de la façon dont les intervenants perçoivent les contrôles en matière de cryptographie dans leur ensemble, pour ce qui est de savoir si les contrôles devraient être renforcés ou assouplis ou si le statu quo a la préférence. Les résultats présentés au tableau 1 indiquent que 78 % des intervenants estiment qu'au moins un certain assouplissement des contrôles est justifié. Les 14 % d'intervenants qui croient que des mesures plus sévères sont justifiées représentent tous le groupe Application de la loi/sécurité nationale. Selon 8 % des intervenants, le statu quo est acceptable, dans l'ensemble.

Tableau 1 : Position d'ensemble au sujet des contrôles en matière de cryptographie

Groupe d'intervenants	N. total de réponses	Plus de contrôles	Moins de contrôles	Statu quo
Particuliers	45	0	43	2
Assoc. industrielles	5	0	4	1
Application de la loi	15	15	0	0
Défenseurs de la protection de la vie privée / des droits de la personne	5	0	5	0
Fournisseurs de matériel / de logiciels	12	0	11	1
Entreprise de télécommunications et associations	4	0	4	0
Universitaires	14	0	12	2
Consultants	5	0	4	1
Secteur public	0	0	0	2
Autres	2	0	0	0
Total	107	15	83	9
Pourcentage		14 %	78 %	8 %

Chiffrement des données stockées

On trouvera au tableau 2 les résultats des réponses aux options en matière de politique suggérées en ce qui a trait au chiffrement des données stockées.

Les options suggérées étaient le libre-jeu du marché; l'adoption de normes minimales; l'accès obligatoire.

Ici, 52 % des intervenants croient que le libre jeu du marché est la meilleure approche; 29 % (57 % des particuliers) préféreraient qu'il n'y ait aucun contrôle, alors que 12 % (appartenant tous au groupe Application de la loi/sécurité nationale) veulent un accès obligatoire; enfin, seulement 6 % optent en faveur de normes minimales. De plus, trois intervenants signalent qu'ils sont opposés à l'option 3 (accès obligatoire) mais ils ne font état d'aucune autre préférence.

Tableau 2 : Chiffrement des données stockées

Groupe d'intervenants	Total	Libre jeu du marché	Normes minimales	Accès obligatoire	Aucun contrôle	Autre préférence
Particuliers	51	19	2	0	29	0
Assoc. industrielles	4	3	1	0	0	0
Application de la loi	16	0	1	14	0	1*
Défenseurs de la protection de la vie privée / des droits de la personne	5	3	0	0	2	0
Fournisseurs de matériel / de logiciels	12	10	1	0	1	0
Entreprises de télécommunications et associations	5	5	0	0	0	0
Universitaires	14	13	1	0	0	0
Consultants	5	3	0	0	1	0
Secteur public	2	2	0	0	0	0
Autres	4	3	0	0	1	0
Total	118	61	7	14	34	1
Pourcentage		52 %	6 %	12 %	29 %	1 %

Exceptions : 3 intervenants indiquent « pas l'option 3 ».
* Des répondants suggèrent l'utilisation d'une forme standard de chiffrement. Ainsi, la clé de déchiffrement pourrait être mise à la disposition des autorités munies d'une autorisation du tribunal.

Chiffrement des communications en temps réel

On trouvera au tableau 3 les résultats des réponses aux options en matière de politique suggérées en ce qui concerne le chiffrement des communications en temps réel.

Les options suggérées étaient : ordonnances d'aide et conditions sélectives pour l'obtention d'une licence (statu quo); obligations imposées à toutes les entreprises de télécommunications; contrôles obligatoires.

Selon 43 % des intervenants, il n'est pas nécessaire d'apporter des modifications aux procédures actuelles (c.-à-d. aux ordonnances d'aide et aux conditions sélectives pour l'obtention d'une licence); 25 % (49 % dans le groupe des particuliers) indiquent qu'il ne devrait y avoir aucun contrôle quel qu'il soit; 11 % (appartenant tous au groupe Application de la loi/sécurité nationale) veulent des contrôles obligatoires; 6 % veulent que l'on impose des obligations aux entreprises de télécommunications; enfin, 5 % suggèrent d'autres options. Chiffre significatif, dans les réponses à cette question, 12 % des intervenants s'opposent explicitement soit à des contrôles obligatoires soit à l'imposition d'obligations aux entreprises de télécommunications (il s'agit d'intervenants qui ont refusé de choisir l'une des options précisées mais qui ont indiqué que les options 2 et 3 étaient inacceptables).

(Voir tableau 3 à la page suivante)

Tableau 3 : Communications en temps réel

Groupe d'intervenants	Total	Statu quo	Obligations pour les entreprises de télécomm.	Accès obligatoire	Pas de contrôle	Autre préférence*
Particuliers	47	19.5	3.5	0	23	1
Assoc. industrielles	5	4	0	0	0	0
Application de la loi[1]	16	0	2.5	12.5	0	1
Défenseurs de la protection de la vie privée / des droits de la personne	5	2.5	0	0	2.5	0
Fournisseurs de matériel / de logiciels	10	7	0	0	1	1
Entreprises de télécomm. et assoc.	5	5	0	0	0	0
Universitaires	14	4	1	0	0	0
Consultants	4	1	0	0	1	2
Secteur public	2	2	0	0	0	0
Autres	2	2	0	0	0	0
Total	110	47	7	12.5	27.5	5
Pourcentage		43 %	6 %	11 %	25 %	5 %

Exceptions : 13 intervenants ont dit « pas l'option 3 » ou « ni l'option 2 ni l'option 3 ».

* Les suggestions proposées dans les autres préférences comprennent l'intégration de dispositions relatives à l'accès légitime dans toutes les applications touchant des transactions à clé publique et à clé de session, assortie d'un appui à l'adoption, au Canada, de mesures législatives du type de celles qui régissent la CALEA; l'accès non obligatoire, avec trois types de services — le chiffrement local, le chiffrement par l'entreprise de télécommunications ou l'absence de chiffrement; le recours à la citation à comparaître pour obtenir de l'information; enfin, le rejet des options énumérées, sans présentation de solutions de rechange mais sans qu'il n'y ait en fait d'opposition à la notion d'accès aux fins de l'application de la loi.

1. Lorsqu'une réponse d'un organisme d'application de la loi ne fait qu'endosser la résolution de l'Association canadienne des chefs de police (annexe A), cette réponse a été interprétée comme étant favorable à des contrôles obligatoires, parce que la résolution demande l'établissement d'un régime de récupération obligatoire des clés pour permettre l'accès aux fins de l'application de la loi; des mesures législatives pour obliger les fournisseurs de services de chiffrement à percer le chiffrement en temps réel pour permettre l'accès aux fins de l'application de la loi; et des mesures législatives pour que les fabricants de services de communications, les fournisseurs de services et les opérateurs de réseaux donnent l'accès aux communications, aux fins de l'application de la loi.

Nota : Lorsqu'une réponse indique que l'une ou l'autre de deux options est acceptable, p. ex., les obligations faites aux entreprises de télécommunications ou l'accès obligatoire, on a ajouté 0,5 point à chaque option.

Contrôle des exportations

Le tableau 4 indique les résultats des réponses aux options en matière de politique suggérées en ce qui concerne le contrôle des exportations.

Les options suivantes ont été proposées : l'assouplissement des contrôles; le maintien de la politique actuelle; l'élargissement des contrôles.

Parmi ceux qui ont répondu à la question concernant le contrôle des exportations, 88 % se montrent favorables à un assouplissement des contrôles (71 %) ou à une absence totale de contrôles (17 %); 6 % optent pour le statu quo et 1 % (qui représente une seule réponse d'un organisme d'application de la loi) veut précisément un élargissement des contrôles.

Tableau 4 : Contrôle des exportations

Groupe d'intervenants	Total	Assouplisse-ment	Statu quo	Élargisseme nt	Pas de contrôles	Autre préférence*
Particuliers	26	16	0	0	10	0
Assoc. industrielles	5	4	0	0	0	1
Application de la loi	4	0	1	1	0	2
Défenseurs de la protection de la vie privée / des droits de la personne	4	3	0	0	1	0
Fournisseurs de matériel / de logiciels	11	10	1	0	0	0
Entreprises de télécommunications et associations	4	4	0	0	0	0
Universitaires	12	10	1	0	0	1
Consultants	5	3	1	0	1	0
Secteur public	0	0	0	0	0	0
Autres	1	1	0	0	0	0
Total	72	51	4	1	12	4
Pourcentage		71 %	6 %	1 %	17 %	6 %

* Une réponse ne présente pas d'opinion mais indique que les auteurs seraient favorables à une décision du gouvernement fédéral concernant le contrôle des exportations; un intervenant déclare que la libre circulation des produits entre le Canada et les États-Unis est essentielle à ses fins; un autre dit que nous ne devrions pas

apporter de modifications susceptibles d'entraîner un déphasage entre le Canada et les États-Unis; enfin, un intéressé s'oppose à toute limitation additionnelle des exportations et rejette la suggestion selon laquelle on pourrait imposer des limites à l'exportation de produits ne permettant pas la récupération des clés.

Partie 2 : Examen des réponses narratives

Observations générales

D'après les commentaires, les intervenants reconnaissent largement la nécessité d'une cryptographie robuste tant à des fins d'affaires qu'à des fins personnelles. Ceux-ci font observer qu'en plus de s'en servir pour le commerce électronique, la prestation de services électroniques et les utilisations relatives à la protection des renseignements personnels, les entreprises en ont besoin pour se protéger contre l'espionnage industriel. Un certain nombre d'intervenants provenant d'horizons divers s'inquiètent de l'effet que les propositions de politiques pourraient avoir sur le commerce électronique et la prestation de services. Un fournisseur souligne que la politique en matière de cryptographie doit appuyer et non entraver les objectifs en matière de prestation de services électroniques. Un certain nombre d'organismes d'application de la loi reconnaissent l'importance de la cryptographie pour le commerce électronique mais servent une mise en garde contre l'utilisation du chiffrement comme écran de protection pour les activités criminelles. Un certain nombre d'intervenants font valoir la nécessité d'éviter l'élaboration d'une politique inapplicable ou d'une politique qui ne réglementerait que les citoyens respectueux des lois.

Douze réponses soulignent qu'il serait futile d'essayer d'imposer des contrôles à l'importation ou à l'utilisation de la cryptographie robuste, puisqu'on peut déjà se procurer librement ce genre de produit un peu partout. Nombreux sont ceux qui rappellent que les criminels auront toujours accès à la cryptographie robuste, que l'utilisation de celle-ci fasse ou non l'objet de restrictions. La disponibilité de techniques non cryptographiques permettant d'assurer la confidentialité est une autre question que les intervenants mentionnent souvent.

Une association qui se consacre à la protection de la vie privée énumère un certain nombre de points qu'elle considère comme étant des erreurs ou des omissions dans le document de travail. Parmi ceux-ci figurent le risque de devoir se fier à un chiffrement ou à des systèmes faibles lorsque les clés doivent être mises à la disposition d'un tiers; les questions de responsabilité; l'impossibilité de détecter la méthode de chiffrement ou même de savoir s'il y a effectivement eu chiffrement; l'omission de toute preuve concrète que l'utilisation du chiffrement a toujours été un obstacle véritable à l'application de la loi dans des cas précis; enfin, l'omission d'exemples bien connus de surveillance abusive et de non-respect de la protection des renseignements personnels.

Un certain nombre d'intervenants font des remarques à propos de la promotion que font les États-Unis de leurs intérêts sur le plan de la politique en matière de cryptographie. Dix intervenants craignent que le Canada se contente de suivre les orientations de la politique américaine en matière de cryptographie et déclarent que cette attitude est inacceptable.

Récupération obligatoire des clés et problèmes relatifs à l'entiercement des clés

Un grand nombre de réponses traitent du manque de réalisme de toute forme de récupération obligatoire des clés ou de dépôt des clés en mains tierces. Cinquante-quatre d'entre elles contiennent des commentaires précis dans lesquels les auteurs s'opposent avec insistance à la récupération obligatoire des clés ou à l'entiercement des clés. De ce nombre, 26 proviennent de particuliers, 5 d'associations industrielles, 4 de fournisseurs, 1 d'une entreprise de télécommunications ou d'une association de télécommunicateurs, 14 du milieu universitaire et 4 d'autres groupes. Seuls les organismes d'application de la loi se montrent favorables à des contrôles additionnels qui permettraient l'accès obligatoire à des données stockées chiffrées. Tout en appuyant la résolution de l'Association canadienne des chefs de police, un organisme d'application de la loi fait observer que l'accès obligatoire constitue une politique restrictive et que cela ne fonctionnera pas. La vaste majorité des intervenants rejettent les contrôles de ce genre. Voici quelques-unes des raisons qu'ils invoquent :

- toute sorte de récupération des clés à des fins d'application de la loi créerait des points de vulnérabilité et affaiblirait la valeur du chiffrement;
- les systèmes de récupération des clés sont moins sécuritaires, plus coûteux et plus difficiles à utiliser;
- on peut se soustraire aux exigences relatives à la récupération des clés;
- le double chiffrement peut être utilisé pour faire échec aux objectifs relatifs à l'entiercement des clés;
- on peut se servir d'algorithmes non standard;
- toute infrastructure de récupération obligatoire des clés sera limitée dans son application;
- le coût d'établissement et de fonctionnement d'une infrastructure de récupération des clés serait élevé et aurait des répercussions négatives sur la compétitivité des entreprises;
- la récupération des clés n'est pas possible pour le type de chiffrement robuste dont on se sert dans le cas des cartes à puce.

Une association industrielle fait observer qu'à l'heure actuelle, il n'y a pas de loi qui prescrive le mode de stockage des données physiques et que les données électroniques ne devraient pas être traitées différemment.

Cinq intervenants font observer que toute tentative de rendre obligatoire le déchiffrement « par la porte d'en arrière » dans les produits cryptographiques canadiens dissuaderait les acheteurs étrangers et désavantagerait les exportateurs canadiens.

Treize réponses comportent des commentaires concernant les points de vulnérabilité additionnels qui seraient introduits par l'intermédiaire d'un système d'entiercement des clés et le danger que les clés confiées à un dépositaire soient utilisées à mauvais escient.

L'une des entreprises de télécommunications invite instamment le Canada à adopter une approche du chiffrement robuste axée sur le marché, étant donné que la récupération obligatoire des clés nous déphaserait par rapport à bon nombre de nos partenaires sur la scène internationale.

Un autre point mentionné fréquemment en ce qui a trait aux contrôles au Canada est qu'on ne dissuadera pas ceux qui veulent enfreindre la loi en imposant, par voie législative, l'utilisation de la cryptographie assortie de dispositions d'accès obligatoire. Les terroristes et les criminels internationaux ont accès à la technologie du chiffrement sur le marché mondial. Les Canadiens ne devraient pas être empêchés de se protéger eux-mêmes. Les contrôles sur l'utilisation au pays sont largement perçus comme étant discriminatoires à l'égard de l'honnête citoyen.

Plusieurs intervenants soulignent qu'il est possible de dissimuler de l'information à l'aide de techniques autres que la cryptographie, telles que la stéganographie, la communications en langage obscur ainsi que le *chaffing/winnowing*.

Accès aux données stockées

Il est généralement reconnu que certaines entreprises doivent prévoir la récupération des clés et la sauvegarde des données pour leurs propres besoins, mais les intervenants ne manquent pas de fermeté quand ils affirment que cela devrait être considéré comme une question interne aux entreprises et non comme quelque chose qui devrait être imposé par l'État. À maintes reprises, ils déclarent que l'on ne devrait pas se servir des besoins des entreprises à ce chapitre comme prétexte pour rendre l'accès obligatoire aux fins de l'application de la loi. Les réponses des entreprises indiquent clairement que ces dernières coopèrent actuellement en cas de demande d'accès légalement autorisée et qu'elles continueront de le faire; toutefois, les entreprises ne veulent pas que l'État leur dise comment s'occuper de leurs affaires.

Un certain nombre d'intervenants laissent entendre que l'on devrait se fier au fait que les entreprises sont déjà tenues de conserver certains types de dossiers à des fins de vérification et que cela devrait suffire.

Récupération des données de télécommunications en temps réel

Dix des réponses (entre autres celles de trois entreprises de télécommunications ou associations de télécommunicateurs, de trois associations et d'un organisme d'application de la loi) font spécifiquement référence à l'impossibilité de demander aux entreprises de télécommunications ou aux fournisseurs de services Internet de déchiffrer des messages qui ont été chiffrés à l'extérieur du réseau de télécommunicateurs. Toutes les entreprises de télécommunications et associations de télécommunicateurs et deux des associations industrielles déclarent que les méthodes existantes dont disposent les organismes d'application de la loi sont suffisantes et qu'aucune mesure additionnelle n'est justifiée.

Trois associations de télécommunicateurs et un fournisseur protestent en disant que la mise au point d'une infrastructure destinée à appuyer le déchiffrement rapide des communications en temps réel serait extrêmement coûteuse et pourrait s'élever à des centaines de millions de dollars. Deux des intervenants (une entreprise de télécommunications et une association) prétendent que la capacité de déchiffrement rapide et universelle jetterait un froid sur l'expansion du commerce électronique, et une des entreprises de télécommunications fait observer que cela s'étendrait à la mise au point de nouvelles technologies de chiffrement. Un des commissaires à la protection de la vie privée utilise aussi l'expression *jeter un froid*, lorsqu'il fait allusion aux contrôles obligatoires sur l'utilisation du chiffrement pour les communications en temps réel, étant donné que « la surveillance secrète et l'accès subreptice aux clés privées créerait les conditions d'une société de surveillance ».

Plusieurs intervenants rappellent que les entreprises de télécommunications ne gardent pas de copie de l'information qui circule sur leur réseau. L'obligation de conserver des clés de session représenterait un fardeau considérable et contreviendrait vraisemblablement à la *Loi sur les télécommunications*, laquelle exige des entreprises de télécommunications qu'elles transportent le trafic téléphonique de leurs clients sans s'ingérer ni dans la forme ni dans le contenu qu'il prend.

Une entreprise de télécommunications indique dans sa réponse que le droit pénal n'a jamais permis aux autorités de surveiller *toutes* les communications criminelles ni de saisir *toute* l'information criminelle pertinente.

On note également dans les observations reçues que les entreprises ont peut-être leurs propres exigences relatives à la récupération des clés dans le cas des données stockées, mais qu'il est rare qu'elles aient une telle exigence dans le cas des communications en temps réel, si tant est qu'elles en aient.

Questions de coût

Il est généralement admis par les intervenants que toute forme de disposition concernant l'accès obligatoire, d'infrastructure de récupération des clés ou d'amélioration dans les dispositions relatives à l'accès des organismes d'application de la loi sera très coûteuse. En tout, 21 réponses, dont certaines venant d'organismes d'application de la loi, mentionnent le coût élevé et plusieurs intervenants, entre autres deux entreprises de télécommunications ou associations de télécommunicateurs, font observer que le coût que la réglementation relative à la récupération des clés imposera aux entreprises ne permettra plus au Canada de soutenir la concurrence internationale.

Qui devrait assumer ces coûts? Tous les groupes expriment leur avis à ce sujet. Ces opinions peuvent se résumer collectivement en deux mots : « pas nous ». Certaines réponses des organismes d'application de la loi laissent entendre que les entreprises de télécommunications, les fournisseurs ou les abonnés devraient assumer les coûts; par contre, selon certains particuliers, certaines entreprises et certaines entreprises de

télécommunications ou associations de télécommunicateurs, ce sont ceux qui exigent le service (c.-à-d. l'État ou les organismes d'application de la loi) qui devraient payer.

D'autres questions de coût ont été soulevées quant à savoir si l'État a fait son devoir en évaluant les coûts, les avantages et les autres incidences des propositions relatives à la politique en matière de cryptographie. Par exemple, certains font observer que les différences entre les utilisations commerciales du chiffrement et ses utilisations à des fins militaires ou de sécurité n'ont pas été suffisamment définies et que le coût et la facilité d'utilisation ne sont pas les premiers facteurs pris en considération dans le domaine militaire ni dans celui de la sécurité, comme ils le sont dans le contexte commercial. Dans ses observations, une association industrielle presse instamment le gouvernement de ne pas procéder à l'adoption de politiques ou de lois en matière de cryptographie tant qu'un examen indépendant visant à déterminer le coût, les avantages et les risques des options proposées n'aura pas été mené à bien.

Une association industrielle soulève la question des coûts associés à l'interface entre les infrastructures à clé publique (ICP) du secteur privé et des institutions, d'une part, et l'ICP du gouvernement du Canada, d'autre part, et elle recommande que les coûts soient « raisonnables, transparents et appliqués de manière uniforme à toutes les ICP, tant privées que publiques ».

Questions relatives à la protection des renseignements personnels

Soixante-douze réponses (39 venant de particuliers, 16 du milieu universitaire, 5 des organismes de défense de la protection de la vie privée et des droits de la personne, 4 de fournisseurs, 3 d'entreprises de télécommunications ou d'associations de télécommunicateurs, 3 du secteur public et 2 d'autres sources) contiennent des commentaires à propos des incidences vraisemblablement défavorables pour la population qu'auront les propositions en matière de politique. À elle seule, cette question suscite plus de commentaires particuliers que toute autre. La crainte que les citoyens respectueux des lois soient désavantagés par des propositions visant à répondre aux besoins des organismes d'application de la loi est la question qui préoccupe le plus. Une association de télécommunicateurs fait observer que « les inquiétudes légitimes quant à l'application de la loi ne devraient pas être traitées d'une manière qui limitera dans les faits l'utilisation légitime du chiffrement par les simples citoyens ou qui réduira les avantages dont jouira le secteur privé grâce à l'utilisation du chiffrement robuste ». Une entreprise de télécommunications fait observer qu'« on doit pouvoir démontrer que toute limite à la cryptographie se justifie dans une société libre et démocratique » et que « les mesures destinées à prohiber l'utilisation de produits de chiffrement non accessibles enfreignent le droit des Canadiens de choisir et d'utiliser les mesures qu'ils considèrent pertinentes pour assurer leur propre sécurité ». Une autre association de télécommunicateurs déclare qu'« on ne devrait pas calmer les inquiétudes des organismes d'application de la loi d'une manière qui a pour effet de limiter l'utilisation légitime du chiffrement à des fins privées ».

Dans une lettre collective, 20 groupes internationaux de protection des droits de la personne exposent les raisons pour lesquelles ils s'opposent aux propositions de politique. À leur avis, une telle politique ou une telle loi serait « contraire aux traités internationaux concernant les droits de la personne, dangereuse pour la société canadienne, préjudiciable pour l'économie canadienne et, en fin de compte, simplement inapplicable ».

Un certain nombre d'intervenants insistent sur la distinction entre la confidentialité, dont on a besoin dans les transactions entre les entreprises, et la protection des renseignements personnels, dont on a besoin dans les transactions entre les clients et les fournisseurs de services, la protection des renseignements personnels étant une question de relation plutôt qu'une question de confidentialité. Un particulier indique dans sa réponse que le droit à la protection de la vie privée ne devrait pas impliquer le droit à l'anonymat, et il laisse entendre que ceux qui font du multipostage abusif ou ceux qui postent des pages Web concernant des questions d'affaires ou des questions d'intérêt public ne devraient pas avoir le droit à l'anonymat.

Questions relatives à l'application de la loi

D'après les réponses quantitatives, il semble y avoir une importante division de l'opinion entre le groupe Application de la loi/sécurité nationale et le reste des intervenants au sujet de la question du contrôle de la cryptographie. Ceci est en partie attribuable au fait que bon nombre de réponses des organismes d'application de la loi ne font qu'endosser, sans nuance, la résolution d'août 1997 de l'Association canadienne des chefs de police (annexe A) qui propose, entre autres, l'établissement d'un régime de récupération obligatoire des clés et des mesures législatives exigeant le déchiffrement en temps réel, dans le but de permettre l'accès pour les fins de l'application de la loi. La vaste majorité des autres intervenants rejettent avec vigueur les parties de cette résolution dans lesquelles on propose des contrôles obligatoires ou additionnels sur le chiffrement. Par ailleurs, certaines réponses des organismes d'application de la loi montrent que ces derniers reconnaissent aussi bien les difficultés que pose la cryptographie que la nécessité de trouver une solution acceptable qui réponde aux besoins en matière d'application de la loi sans enfreindre les droits de l'individu. Un organisme d'application de la loi fait observer que, bien que leurs demandes puissent sembler constituer un obstacle au progrès, les organismes d'application de la loi ne cherchent pas à obtenir des moyens accrus de faire des enquêtes ni de nouveaux pouvoirs, mais simplement le rétablissement et le maintien des moyens qu'ils avaient à leur disposition auparavant.

Dans l'ensemble, les auteurs des observations reçues appuient fermement la déclaration d'un intervenant selon laquelle il n'y a pas de consensus populaire, en dehors des milieux chargés de l'application de la loi, quant à la nécessité de réglementer la cryptographie. Dans 46 réponses, on trouve des commentaires selon lesquels leurs auteurs ne croient pas à la nécessité de réglementer la cryptographie et (ou) pensent que les méthodes existantes dont disposent les organismes d'application de la loi pour obtenir de l'information sont suffisantes pour assurer la sécurité publique et la sécurité nationale. Parmi ces réponses, 28 proviennent de particuliers, 5 d'entreprises de télécommunications ou d'associations de

télécommunicateurs, 5 de groupes de défense de la protection de la vie privée, 2 d'associations industrielles et 6 d'autres groupes. D'après une association de télécommunicateurs, « les besoins des utilisateurs, des entreprises de télécommunications et des tiers fournisseurs de commerce électronique sont dans certains cas en conflit direct avec les besoins déclarés des organismes chargés de l'application de la loi et de la sécurité. Un certain nombre d'intervenants, dont un commissaire à la protection de la vie privée, font observer que les organismes d'application de la loi n'ont pas prouvé que les moyens d'interception et de déchiffrement recherchés entraîneront une baisse de la criminalité. De plus, il est clair que bon nombre d'intervenants (46 réponses) estiment que les méthodes dont disposent actuellement les organismes d'application de la loi pour obtenir de l'information sont suffisantes pour leur permettre de continuer à assurer la sécurité du public et la sécurité nationale.

De nombreux intervenants reconnaissent certes la nécessité de trouver une solution aux problèmes posés par la cryptographie robuste en matière d'application de la loi, mais, à maintes reprises, ils soulignent que ce serait manquer de réalisme que d'essayer de contrôler la cryptographie. Par ailleurs, la récupération obligatoire des clés ou les contrôles obligatoires sur les entreprises de télécommunications au-delà des mesures qui existent actuellement ne recueillent pour ainsi dire aucun appui.

Certaines des demandes formulées dans les observations venant des organismes d'application de la loi ne risquent guère de trouver beaucoup d'appui dans le grand public (p. ex., l'obligation d'inscrire tous les citoyens canadiens et tous les immigrants reçus dans un système de récupération des clés et l'affectation d'un mot de passe unique à tous ceux qui s'inscrivent). Par contre, d'autres suggestions de la part des organismes policiers concordent davantage avec la majorité des observations, puisqu'on y reconnaît que le fait d'essayer d'appliquer des contrôles d'accès obligatoire dans le cas des données stockées ou des exigences d'accès obligatoire concernant les entreprises de télécommunications comporte une difficulté technique, un manque de réalisme et des incidences financières. Un petit nombre d'organismes d'application de la loi reconnaissent implicitement dans leurs commentaires que le problème auquel se heurtent ces organismes n'est pas uniquement un problème de cryptographie mais aussi un problème lié à l'évolution rapide de la technologie et à la mise au point de moyens techniques dont on peut abuser. Dans plusieurs contributions, dont un certain nombre proviennent des organismes d'application de la loi eux-mêmes, on fait allusion au fait que les organismes d'application de la loi ne sont pas équipés pour s'attaquer à la technologie actuelle. Les intervenants laissent entendre qu'il faut des outils additionnels, de l'information technique, du soutien technique, plus de ressources pour surveiller et déceler les intrusions ainsi qu'une stratégie nationale pour se tenir au courant de la technologie et pour aider la technologie à tenir promesse, c'est-à-dire à aider plutôt qu'à gêner l'application de la loi.

Plusieurs propositions visant à satisfaire les besoins sur le plan de l'application de la

loi viennent de groupes autres que les organismes d'application de la loi. Mentionnons entre autres le recours aux ordonnances des tribunaux pour obtenir l'accès aux clés; la mise en application des lois existantes sur la remise de l'information; la collecte de renseignements par des moyens autres que l'examen de dossiers chiffrés; l'analyse cryptographique; enfin, l'utilisation de techniques existantes et de techniques nouvelles pour recueillir des données informatisées et autres. Un organisme d'application de la loi recommande, comme solution de rechange aux contrôles obligatoires, l'adoption de normes minimales afin de permettre au gouvernement fédéral de fournir un enseignement, une orientation et une structure concernant l'utilisation et la mise au point de la cryptographie. Un autre organisme d'application de la loi reconnaît quant à lui l'ampleur de la tâche qui consiste à essayer d'appliquer des règles en matière de chiffrement et il recommande que « parallèlement aux initiatives existantes, on mette en oeuvre des stratégies de rechange et qu'on accorde un appui à la mise au point de techniques d'enquête, si le problème déjoue toutes les tentatives de contrôle législatif ». Une association industrielle laisse entendre qu'il devrait y avoir un dialogue permanent entre les fabricants de produits de chiffrement, les utilisateurs et les organismes d'application de la loi, et elle offre d'agir comme hôte d'un tel dialogue.

Dans la résolution de l'Association canadienne des chefs de police, on recommande entre autres la criminalisation de l'utilisation de la cryptographie dans la perpétration d'un crime. Cette recommandation est fréquemment mentionnée dans les observations venant des organismes d'application de la loi. Bien qu'elle ne semble pas recueillir un appui vigoureux auprès des autres intervenants, cette mesure est également proposée par une des associations industrielles.

Contrôle des exportations

Deux questions ressortent très fortement à ce chapitre : d'une part, l'application que l'on fait actuellement des contrôles sur les exportations place le Canada dans une position désavantageuse par rapport à ses concurrents; d'autre part, il est nécessaire de travailler de concert avec la communauté internationale.

Les résultats quantitatifs révèlent que seulement 7 % des intervenants sont en faveur du maintien du statu quo ou de l'élargissement des contrôles à l'exportation. Dans chaque groupe d'intervenants autre que celui des organismes d'application de la loi, la majorité des gens sont en faveur d'un assouplissement des contrôles. (Seulement quatre organismes d'application de la loi ont répondu à la question sur le contrôle des exportations. L'un d'eux est en faveur de l'élargissement des contrôles; un autre est en faveur du statu quo; un troisième choisit de demeurer neutre sur le sujet mais d'appuyer toute initiative ou toute décision de la part du gouvernement fédéral; enfin, le dernier reconnaît l'existence de certains arguments en faveur d'un assouplissement, mais il invite instamment à la prudence et constate qu'il faut demeurer aligné sur les États-Unis.)

Vingt-quatre réponses (entre autres celles de trois associations industrielles, de quatre

entreprises de télécommunications ou associations de télécommunicateurs et de huit fournisseurs) comportent des commentaires au sujet des effets négatifs des restrictions actuelles sur l'exportation de produits cryptographiques. On y insiste en particulier sur le point selon lequel le contrôle des exportations met les fournisseurs canadiens de produits cryptographiques dans une situation désavantageuse par rapport à leurs concurrents. Bon nombre de ceux qui plaident en faveur d'un assouplissement des contrôles soulignent aussi la nécessité de continuer à travailler avec la communauté internationale dans ce dossier, mais, comme on le fait remarquer dans plusieurs réponses, les dispositions de l'Arrangement de Wassenaar sont interprétées de façon souple par certains autres pays. Dans un des mémoires, on décrit avec beaucoup de précision l'exemple des États-Unis qui donnent leur approbation générale à certaines sociétés pour qu'elles exportent des produits de cryptographie robuste. L'Allemagne, la Suisse et la République d'Irlande sont également mentionnés comme étant des pays qui permettent aux entreprises d'exporter librement des produits cryptographiques. Les intervenants constatent que le Canada néglige de profiter de la flexibilité que lui permet l'Arrangement de Wassenaar.

Bien que l'élimination des contrôles à l'exportation jouisse dans l'ensemble d'une nette préférence, les intervenants suggèrent fortement que le Canada profite au maximum de la souplesse que lui permet l'Arrangement de Wassenaar pour libéraliser les contrôles le plus possible, si les contrôles des exportations doivent demeurer en vigueur.

Dans deux des réponses, on soutient que les produits cryptographiques commerciaux ne devraient pas être assujettis aux contrôles sur la technologie militaire et l'on fait observer que les produits cryptographiques sont des outils commerciaux importants qui sont maintenant utilisés par les entreprises plus que par les militaires.

En ce qui concerne les règles d'exportation, on suggère entre autres comme option de donner une approbation générale aux exportations de produits comportant une clé de chiffrement d'une longueur maximale déterminée et de procéder au cas par cas pour l'approbation de clés de longueur supérieure à la longueur spécifiée (on recommande des clés de 128 bits pour le chiffrement symétrique et des clés de 1 024 bits pour le chiffrement asymétrique). Autre suggestion : que l'on cesse d'exercer un contrôle sur les exportations, sauf dans le cas d'embargos particuliers à certains pays. Il est également suggéré que les logiciels et le matériel informatique tant du domaine public que du marché de masse soient exempts de contrôles; que l'État donne son approbation générale à l'exportation d'un produit plutôt que d'exiger un permis d'exportation à chaque occasion; et que les exportateurs canadiens soient autorisés à exporter des produits de calibre semblable à ceux des autres pays, dans les mêmes proportions que ceux-ci.

Nécessité de traiter les fournisseurs et les entreprises de télécommunications sur un

pied d'égalité

Bien que les intervenants s'opposent en général aux contrôles obligatoires et aux règlements, ils font souvent observer que toute décision en matière de politique doit être neutre du point de vue technologique et que si l'on impose certaines obligations aux fournisseurs, tous doivent être traités sur un pied d'égalité.

En particulier, trois entreprises de télécommunications ou associations de télécommunicateurs recommandent avec insistance que toutes les entreprises de télécommunications et tous les fournisseurs de services – et non seulement ceux et celles qui sont considérés comme faisant partie du réseau téléphonique commuté public – soient visés par les ordonnances d'aide et par l'obligation de coopérer avec les organismes d'application de la loi. Un organisme d'application de la loi constate aussi qu'il faut traiter tous les membres de l'industrie sur un pied d'égalité dans l'application de l'accès obligatoire et de l'interception légitime. Un intervenant déclare que les contrôles sélectifs et la délivrance de licences (comme les conditions pour l'obtention d'une licence imposées aux entreprises de télécommunications sans fil) créent une distorsion sur le marché et font peser un fardeau injuste sur certains fournisseurs. Comme le fait remarquer un intervenant, « étant donné que l'industrie des télécommunications s'ouvre de plus en plus à la concurrence, il ne serait pas judicieux pour le gouvernement de créer une politique qui répartirait le fardeau du respect des directives en matière de politique d'une manière qui désavantage un type de fournisseur de services par rapport à un autre ».

Les associations de télécommunicateurs et deux fournisseurs recommandent aussi que tout contrôle de l'utilisation commerciale du chiffrement s'applique à tous les secteurs de l'économie.

Il est aussi question de traitement égal lorsqu'il s'agit de restrictions à l'exportation. Un fournisseur recommande en effet avec insistance que l'on accorde le même traitement au matériel de cryptographie destiné au marché de masse et généralement offert sur le marché qu'aux logiciels de cryptographie.

Questions relatives à la législation, à la réglementation et à la Charte des droits

Dix-neuf intervenants (14 du milieu universitaire, 2 d'entreprises de télécommunications ou d'associations de télécommunicateurs, 2 de groupes de défense de la protection de la vie privée et 1 d'un commissaire à la protection de la vie privée) craignent que les propositions en matière de politique n'enfreignent la *Charte des droits et libertés* et (ou) des lois, dont la *Loi sur les télécommunications*. Certains organismes d'application de la loi font observer que toute législation éventuelle doit être en harmonie avec la *Charte des droits et libertés*. Un organisme d'application de la loi laisse entendre que les arguments

présentés à propos du droit qu'ont les Canadiens de jouir de la protection de la vie privée et de la liberté d'expression en vertu de la *Charte* ne devraient pas faire problème, parce que l'interception exige une justification et l'approbation préalable des tribunaux.

Les questions de responsabilité sont soulevées dans cinq contributions, en particulier la responsabilité des tiers en ce qui a trait à la divulgation non autorisée d'information confidentielle, comme les clés. On y fait également mention des questions de responsabilité qui se posent si les sociétés sont tenues de garder de l'information confidentielle mais sont contraintes par la loi d'utiliser seulement un chiffrement faible ou un chiffrement accessible à un tiers.

Un organisme d'application de la loi fait observer qu'il n'y a pas de fondement juridique particulier dans le *Code criminel* qui oblige le possesseur d'une clé cryptographique ou d'un mot de passe à divulguer de l'information. Le même organisme rappelle également que les modifications apportées récemment au *Code criminel* l'ont été en réaction à des problèmes, et qu'en conséquence, il est difficile pour les organismes d'application de la loi de demeurer à la fine pointe de la technologie.

Un certain nombre d'intervenants recommandent instamment que toute mesure prise par le gouvernement soit proportionnelle à la portée et à l'importance du problème, et que l'on tienne compte du coût probable de la réaction et de l'effet probable, tant sur la population cible (p. ex., les criminels) que sur toutes les autres (milieux d'affaires, fournisseurs de services, fournisseurs de logiciels et d'équipement, utilisateurs et grand public en général). Un certain nombre de réponses de particuliers et de défenseurs de la protection de la vie privée ou des droits de la personne s'interrogent sur la nécessité de limiter les droits relatifs à la protection des renseignements personnels de tous les Canadiens sur la base d'hypothèses et de suppositions formulées par des organismes chargés de l'application de la loi ou de la sécurité nationale, quand il n'y a pas de preuve réelle que la cryptographie entrave sérieusement les enquêtes policières. Une association industrielle souligne que les exigences en matière d'application de la loi et de sécurité nationale qui limitent l'application de la cryptographie robuste auraient non seulement pour effet de compromettre les programmes de sécurité de l'industrie mais ils pourraient aussi entraîner des coûts qui viendraient contrebalancer les avantages du commerce électronique pour le consommateur. Un certain nombre d'auteurs d'observations insistent fortement pour qu'une analyse de rentabilité complète soit effectuée avant que des décisions ne soient prises au sujet de l'une ou l'autre proposition. D'autres recommandent que l'on évite de mettre en place un centre de déchiffrement et de surveillance pour tous les utilisateurs, quand on ne vise qu'un petit nombre d'individus.

Les mémoires venant du secteur public / des commissaires à la vie privée soulignent la

nécessité de faire en sorte que l'infrastructure de chiffrement requise soit sécuritaire et éprouvée. Il faut aussi, selon eux, que la politique en matière de cryptographie oblige les tiers de confiance à respecter des principes et des pratiques stricts en matière de protection des renseignements personnels.

Autres questions

Un certain nombre d'intervenants soulignent que l'on peut faire valoir un argument irréfutable selon lequel l'utilisation généralisée de la cryptographie robuste peut faire progresser l'application efficace de la loi plus qu'elle ne peut permettre à certains individus et à certaines organisations de communiquer en privé à propos d'actes illégaux.

Six intervenants recommandent instamment que la politique et les règles en matière de cryptographie tiennent complètement compte des normes publiques, internationales. Dans ses observations, une association industrielle fait référence à l'ensemble de mesures législatives disparates qui existent aux États-Unis en matière de signature numérique et elle déclare qu'il faut des normes au Canada afin d'éviter que la même chose ne se produise.

Une association souligne que la prudence est de rigueur dans l'utilisation de produits cryptographiques importés. Ceux-ci pourraient en effet comporter des caractéristiques non documentées permettant à des tiers d'accéder subrepticement aux transactions d'un utilisateur. L'association suggère qu'il y ait une certaine forme d'évaluation et d'homologation des produits cryptographiques.

Une entreprise recommande pour sa part que les sociétés qui ont une vaste clientèle soient autorisées à servir d'autorité de certification.

Conclusions et mesures de suivi possibles

Un certain nombre de messages vigoureux ressortent des commentaires et des réponses. Il est clairement indiqué dans la majorité des réponses et les justifications qui les accompagnent que :

- les contrôles obligatoires sur l'utilisation ou l'importation de moyens de chiffrement sont inacceptables pour les affaires, l'industrie, le commerce, les défenseurs de la protection de la vie privée et des droits de la personne, les universitaires et les particuliers, et il en va de même de toute forme d'entiercement des clés ou de système de récupération obligatoire des clés;

- rendre obligatoire l'accès aux données déchiffrées des communications en temps réel ne peut se faire qu'à grands frais; de plus, il s'agit d'une mesure qui comporte un risque important pour la compétitivité du Canada et la protection des renseignements personnels;
- l'adoption de nouvelles mesures destinées à donner accès à des données stockées

chiffrées est généralement considéré comme injustifié et inutile;

- l'application actuelle des contrôles à l'exportation ne concorde pas avec les règles internationales et elle désavantage les entreprises canadiennes;

- les intervenants préfèrent les solutions déterminées par le marché à d'autres solutions, pour ce qui est des options en matière de politique qui ont été énumérées;

- la cryptographie robuste et d'autres innovations technologiques créent de sérieuses difficultés aux organismes d'application de la loi dans l'utilisation de certaines techniques d'enquête classiques;

- les intervenants craignent sérieusement que les mesures découlant des propositions actuelles en matière de politique aient un impact défavorable sur la protection des renseignements personnels et, en particulier, que les citoyens respectueux des lois soient désavantagés par des propositions destinées à répondre aux besoins des organismes d'application de la loi.

On trouvera ci-dessous un résumé des mesures possibles suggérées dans les observations reçues dans le but de répondre aux besoins des organismes d'application de la loi, des entreprises, de l'industrie, du commerce et des simples citoyens :

- adoption d'une loi fédérale pour faire de l'utilisation du chiffrement une infraction, si cette utilisation a pour but de dissimuler l'activité criminelle;

- modification du *Code criminel* pour que le refus de communiquer une clé de chiffrement ou de fournir de l'information en texte clair en réponse à une ordonnance du tribunal devienne une infraction;

- adoption d'une loi fédérale pour légitimer et reconnaître l'utilisation des signatures numériques;

- adoption d'une loi fédérale pour protéger l'utilisateur de la cryptographie contre la divulgation, par des tiers, de sa clé ou d'autres renseignements protégés sans que les tiers n'y soient autorisés;

- assistance aux organismes d'application de la loi afin de leur permettre de se tenir au courant de l'évolution de la technologie d'une manière pratique et réaliste, ce qui les aidera à faire respecter la loi;

- établissement d'un dialogue permanent entre les organismes d'application de la loi, les fournisseurs de services, les fournisseurs de logiciels, de matériel informatique et de produits cryptographiques pour aider les organismes d'application de la loi

dans l'exécution de leur travail;

- assouplissement progressif des restrictions à l'exportation, conformément aux obligations du Canada aux termes de l'Arrangement de Wassenaar;

- encouragement actif de l'utilisation légitime de la cryptographie robuste comme moyen d'inspirer confiance envers le commerce électronique et la prestation de services électroniques sécuritaires, et comme moyen de réduire le crime électronique.

Partie 3 : Suggestions en vue d'accélérer le déploiement du commerce électronique sécuritaire

Bien que de nombreux intervenants aient choisi de limiter leurs remarques aux questions relatives à la politique en matière de cryptographie, un certain nombre d'observations reçues contiennent des réponses à l'invitation de commenter les mesures destinées à accélérer le déploiement du commerce électronique sécuritaire. Les suggestions ci-dessous sont tirées d'observations dont les auteurs ont choisi de faire des commentaires à ce sujet.

Problèmes juridiques

1. Établir une loi qui soit formulée de manière à créer un cadre national permettant de reconnaître la validité des méthodes d'authentification électroniques sur le même pied que les signatures écrites.

2. En facilitant l'admissibilité des documents produits par ordinateur à des fins de preuve, faire en sorte que les lois contribuent à l'utilisation des méthodes électroniques (comme les signatures numériques) au lieu d'imposer des systèmes de réglementation onéreux et compliqués comme l'ont fait certains États.

3. Favoriser un contexte dans lequel le marché, grâce à des plans de normalisation nationaux et internationaux, sera encouragé à mettre au point des procédures détaillées afin d'étayer la fiabilité des systèmes d'authentification.

4. S'employer à clarifier les règles relatives à la responsabilité, en particulier celles qui sont associées aux signatures numériques et à la divulgation non autorisée de l'information par des tiers.

Tiers de confiance

1. Adopter une approche axée sur le marché pour l'établissement des services d'autorité de certification. À ce stade-ci, un régime de licence serait un fardeau tant pour les utilisateurs du commerce électronique que pour l'infrastructure en émergence. (Précisons que certaines institutions existantes telles que les institutions financières, le Bureau des passeports et le bureau de poste semblent avoir les qualifications requises pour agir comme autorités de certification.)

2. Reconnaître qu'en ce qui concerne les autorités de certification, le meilleur moyen de parvenir à des pratiques d'affaires efficaces, qui auront des répercussions minimales sur les coûts et l'efficacité, consiste à encourager le secteur privé à mettre au point des méthodes pour servir d'autorité de certification, en consultation avec le secteur public.

Prédication par l'exemple

1. Le gouvernement devrait jouer un rôle de chef de file comme utilisateur modèle du commerce électronique et de la prestation de services électroniques; il devrait également jouer un rôle majeur en faisant publiquement la promotion de ces services et en enseignant aux consommateurs à s'en servir.

2. Le gouvernement fédéral devrait élargir son rôle comme utilisateur modèle d'Internet et fournisseur de services en ligne, comme la transmission électronique des déclarations, en accélérant la prestation de services en ligne et en élargissant la gamme des services en ligne qui sont offerts (par exemple, on ne trouve pas encore de formulaires électroniques sur Internet) et en permettant aux citoyens de communiquer directement avec les ministères.

Sécurité du commerce électronique

1. Reconnaître que la cryptographie est seulement un élément de l'infrastructure de sécurité qui est indispensable aux services gouvernementaux en ligne. Il est essentiel que l'information stockée localement soit gardée en toute sûreté, à l'abri de l'intrusion, et récupérable en cas de panne ou de désastre.

2. L'application des produits et des services cryptographiques aura un effet habilitant sur tous les secteurs de l'activité économique et sociale. Tant que le chiffrement ne sera pas largement accessible ni largement déployé, on aura beaucoup de mal à créer de nouvelles formes d'entreprises, plus compétitives. La cryptographie robuste est nécessaire au succès du commerce électronique, et son utilisation devrait être encouragée.

3. Veiller à ce que les politiques soient basées sur des normes publiques, internationales.

4. Veiller à ce que les protocoles, les logiciels et les algorithmes de chiffrement soient bien documentés et librement accessibles; ainsi, les utilisateurs qui s'y connaissent pourront en vérifier eux-mêmes la robustesse et la qualité. Éviter les restrictions touchant la conception, la création ou la mise en oeuvre de la cryptographie robuste.

5. Envisager l'établissement ou la reconnaissance d'un centre d'évaluation indépendant qui fournira aux utilisateurs l'assurance que les algorithmes cryptographiques sont solides et fiables.

Rôle de l'État dans la promotion des services électroniques

1. Les consommateurs ne sont pas encore persuadés qu'ils peuvent faire des affaires sur Internet de façon sécuritaire. Le gouvernement doit travailler avec le secteur privé à la mise au point de procédures de sécurité efficaces et renseigner le public au sujet de ces procédures. S'employer à inspirer la confiance aux consommateurs.

2. Éviter l'excès de réglementation, qui étouffe le développement de la technologie et empêche le consommateur d'avoir confiance dans le commerce électronique.

3. Faire en sorte que les politiques en matière de cryptographie n'entravent pas à l'excès la capacité des Canadiens de protéger la confidentialité et l'intégrité de leurs communications électroniques.

4. Éviter les mesures qui augmenteraient excessivement le coût des transactions électroniques.

5. Appuyer et aider activement l'industrie canadienne de la TI à fournir au commerce électronique la sécurité requise.

6. Acquérir des produits et des services canadiens assurant la sécurité de la TI et en faire la promotion.

7. Encourager l'interopérabilité entre les infrastructures de sécurité du gouvernement fédéral (comme l'ICP) et les autres infrastructures de sécurité des secteurs public et privé.

8. Permettre le libre jeu du marché et assurer l'uniformisation des règles du jeu pour l'industrie canadienne de la sécurité des TI.

9. Travailler à faire en sorte que tout le monde ait accès à des services en ligne, et non seulement ceux qui peuvent se permettre d'avoir leur propre ordinateur et leurs propres services Internet.

10. Éviter de forcer les gens à acheter un logiciel commercial particulier ou de passer par des agents particuliers, comme il faut maintenant le faire pour la transmission électronique des déclarations.

11. Veiller à ce que les coûts liés à l'interopérabilité avec les infrastructures de sécurité de l'État soient peu élevés.

Enjeux internationaux

1. Continuer de s'employer à promouvoir le commerce électronique mondial sécuritaire sur les tribunes internationales et à réduire les obstacles au commerce mondial des produits et des services cryptographiques.

Remarques finales

L'analyse présentée dans ce rapport se limite forcément à un aperçu des questions qui reviennent le plus souvent et elle s'accompagne d'un choix subjectif de quelques-uns des points qui ont été mentionnés moins fréquemment. Une telle analyse peut certes offrir une vue d'ensemble de l'ampleur du consensus qui existe, mais elle ne peut pas rendre compte de la richesse du détail ni des idées particulières que contient chacune des réponses, sinon dans une mesure très limitée. Comme nous l'avons indiqué précédemment, chacune des réponses montre que les individus et les organisations qui ont répondu au document de travail d'Industrie Canada ont beaucoup réfléchi et ont fait un effort considérable. Ces contributions fournissent quantité de détails et regorgent d'idées au sujet d'une tâche difficile : l'élaboration d'une politique canadienne en matière de cryptographie qui soit équilibrée. Il faut remercier tous ceux et celles qui ont pris la peine de répondre à ce sujet et qui, d'une certaine façon, contribuent à l'établissement d'un consensus à ce propos.

Annexe A : Résolution de l'Association canadienne des chefs de police, août 1997

Il est résolu que l'association canadienne des chefs de police demande instamment au gouvernement du Canada :

1. d'établir une infrastructure à clé publique exigeant des autorités de certification licenciées et un régime de récupération obligatoire des clés qui donnerait un accès légitime aux clés de chiffrement;

2. d'édicter les lois voulues, y compris des modifications au *Code criminel*, pour faire de l'utilisation du chiffrement aux fins de la perpétration d'un crime une infraction et pour permettre la saisie de tout équipement utilisé à ces fins;

3. d'édicter les lois voulues pour obliger les fournisseurs de services de chiffrement à fournir les services qui permettront de percer le chiffrement en temps réel pour les besoins d'accès légitime des organismes d'application de la loi et des agences de sécurité nationale;

4. d'édicter les lois voulues pour que les fabricants de services de communications, les fournisseurs de services et les opérateurs de réseaux existants et futurs donnent légitimement accès aux communications, sans frais, aux organismes d'application de la loi;

5. de fonder en lois et en politiques l'aide que pourrait fournir le Centre de sécurité des télécommunications aux organismes d'application de la loi et aux agences de sécurité nationale en matière de cryptographie et de technologie semblable utilisée pour commettre une infraction;

6. d'établir des normes gouvernementales pour inspirer la confiance dans l'infrastructure d'information, pour réduire les risques d'utilisation à des fins criminelles ou à d'autres fins contraires aux intérêts du public;

7. d'augmenter le niveau de ressources pour qu'il se fasse plus de recherche et de développement concernant les mesures technologiques et autres, afin de surmonter certains des obstacles que posent la cryptographie et d'autres technologies semblables aux organismes d'application de la loi et aux agences de sécurité nationale.

Annex B : List des mémoires reçus en réponse au document de travail

1) Mémoire des organisations

Action Software International	042
Alliance de Manufacturiers et des Exportateurs du Canada	1-314
Association canadienne de technologie de l'information (ACTI)	153
Association canadienne de technologie de Pointe (ACTP)	125
Associations canadienne de télévision par câble (ACTC)	112
Association canadienne des Télécommunication san fil (ACTS)	166
Association des banquiers canadiens (ABC)	118
Brockville Police	070
British Columbia Civil Liberties Association	139
Canadian Association of Internet Providers	123
Canadain Business Telecommunications Alliance (CBTA)	1-317
Chrysalis-ITS	129
City of Charlettetwon Police Headquarters	063
Commissaire à la protection de la vie privée du Canada	162
Commissaire à l'information et à la protection de la vie privée Ontario, (Ann Cavoukian)	128
Commission d'accès à l'information du Quebec	094
Delta Police Department	160
DMR Consulting Group Inc.	037
Domus Software	126

EWA	168
Edmonton Police Service	171
Electronic Frontier	116
Entrust Technologies	130
Gandalf Graphics Limited	157
Gendarmerie royale du Canada (GRC) (Ottawa)	095
Gendarmerie royale du Canada (GRC)(Ottawa)	097
Gendarmerie royale du Canada (GRC)(Vanier)	1-312
Gendarmerie royale du Canada (GRC)(Victoria, BC)	164
Gendarmerie royale du Canada (GRC)(Whitehorse, Yukon)	115
GT Group Telecom Inc.	031
H&R Block Canada Ltd. (Calgary)	163
Halifax Regional Municipality	169
Hewlett-Packard (Canada)Ltd. (Mississauga)	137
Hyprotech Ltd. (Calgary)	156
Information Technology Laboratory National Institute of Standards and Technology	006
Institute for the Study of Privacy Issues (ISPI)	090
Intelligent Switched Systems	077
IT Management Consultant	013
KPMG	133

La Fédération nationale des associations de consommateurs du Québec et Option consommateurs	143
London Police	093
Manitoba Association for Access and Privacy	124
Metropolitan Toronto Police	142
Microcell Telecom Munications Inc.	136
Mimosa Systems Inc.	146
MIT Lab for Computer Science	046
Motorola Canada Limited	141
Northern Lights College	045
Okiok Data Ltd.	099
Prince Albert Police Service	170
Queens University	101
Regina Police Service	167
Rogers Communications Inc.	152
Royal Newfoundland Constabulary	092
Science, Research and Information Technology (Alberta)	127
Service canadien du renseignement de sécurité	1-311
Société Canadienne des post	1-302
Société Canadienne des post (Produits et services électroniques)	1-308
Stentor Politiques publiques Télécom Inc.	131
Telus Corporation	140

The London School of Economics and Political Science	135
Timestep Corporation	087
Twiggy Design	113
Université de Montréal	144
Université de Toronto	039
Université de Toronto (Department of Electrial and Computer Engineering)	138
Valmet Automation	108
Vancouver Webpages	081
Vidéotron Télécom ltée	1-318
Victoria Police Department	117
Ville de Québec Servic de police	159
Ville de Windsor Service de police	067
Ville de Winnipeg Service de police	047
WinMagic Inc.	098

2) Mémoires des particuliers

Arzumania, Ara	066
Bartel, Mark	056
Bernier, M.V.	058
Caldwell, Joshua	1-310
Chappel, David A.	1-313

Chin, Tony	052
Clayton, Michael J.	079
de Raadt, Theo	002
Darwin, Ian	132
Décarie, Richard	102
Duford, Lee	059
Galloway, Dave	154
Graham, Hugh	121
Gregory, Don W.	091
Harminc, Tony	1-300
Hart, Rob	085
Hayes, Amos	1-301
Hekimian, Hrad	066
Hinke, C.J.	1-315
James, Mark	100
Jeffery, Jim	027
Jeppsson, Jonas	119
Klassen, Arthur N.	078
Kossmann, William	054
Litwyn, Jay	015
Lloyde, William	032

Lynne, Stuart	053
MacGregor, John	060
Macrae, Robin	1-309
Maniscalco, Nick	109
Martin, C.	062
McCutcheon, Mark	151
McElvanney, Matthew	034
Milliken, Peter (House of Commons, Kingston)	172
Narveson, Jan	106
O'Malley, Sarah	155
Perrin, D.B.	040
Pick, Jim	089
Plumb, Marc	107
Quinton, Reg	075
Reid, Robert	103
Robinson, Ken	145
Sampson, Curt	076
Savard, John	104
Schuetz, Marko	110
Smith, Eric S.	1-316
Spencer, Henry	158

Streifling, Jeffrey	073
Tarrant, Keith	035
Tomlin, Gord	042
Taylor, M.	1-303
Tyler, Nicholas	064
Tyson, Al	033
Wilson, Brad	072